HP ProtectTools

お使いになる前に

Bluetooth は、その所有者が所有する商標であり、使用許諾に基づいて Hewlett-Packard Company が使用しています。Intel は米国 Intel Corporation の米国およびその他の国における登録商標であり、使用許諾に基づいて使用しています。Microsoft、Windows、および Windows Vista は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

本書の内容は、将来予告なしに変更されることがあります。HP 製品およびサービスに関する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。

初版：2011 年 1 月

製品番号：638391-291

目次

1 セキュリティの概要

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）ソフトウェアには、コンピューター、ネットワーク、および重要なデータに対する不正アクセスの防止に役立つセキュリティ機能があります。

アプリケーション	機能
HP ProtectTools 管理者コンソール（管理者用）	• アクセスするには、Microsoft® Windows®の管理者権限が必要です • 管理者が設定したモジュールにアクセスできます。ユーザーはこれらのモジュールにはアクセスできません • セキュリティの初期セットアップを行えます。また、すべてのユーザーに適用されるオプションまたは要件を設定できます
HP ProtectTools Security Manager（ユーザー用）	• ユーザーは管理者によって提供されたオプションを設定できます • 管理者は、一部の HP ProtectTools モジュールに対する限定的なコントロールをユーザーに提供できます

コンピューターで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。詳しくは、http://www.hp.com/jp/にアクセスしてください。

注記： このガイドの操作手順は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

HP ProtectTools の機能

以下の表で、HP ProtectTools モジュールの主な機能を詳しく説明します。

モジュール	主要な機能
HP ProtectTools 管理者コンソール（管理者用）	• HP ProtectTools Security Manager セットアップ ウィザードを使用して、セキュリティ レベルおよびセキュリティ ログイン方法を設定します • ユーザーからは非表示になっているオプションを設定します • Device Access Manager およびユーザー アクセスを設定します • 管理者ツールを使用して、HP ProtectTools ユーザーを追加および削除したり、ユーザーの状態を表示したりします
HP ProtectTools Security Manager（ユーザー用）	• パスワードを整理、セットアップ、および変更します • Windows パスワード、指紋、スマート カードなどユーザーの証明情報を設定および変更します • File Sanitizer のシュレッド、ブリーチ（漂白）などの設定を構成します • Device Access Manager の設定を表示します • Computrace for HP ProtectTools を設定します • オプションおよび[バックアップおよび復元]オプションを設定します
Credential Manager for HP ProtectTools（Password Manager（パスワード マネージャー））	• ユーザー名およびパスワードを保存、整理、および保護します • Web サイトおよびプログラムのログオン画面を設定し、すばやく安全にアクセスできるようにします • 入力した Web サイトのユーザー名およびパスワードを Password Manager に保存します。次にこのサイトを表示したときに、Password Manager がユーザー名およびパスワードを自動的に入力して送信します • 強固なパスワードを作成してアカウントのセキュリティを強化します。Password Manager は、この情報を自動的に入力して送信します
Drive Encryption for HP ProtectTools（一部のモデルのみ）	• ハードドライブをボリューム全体にわたって完全に暗号化します • データの暗号化解除やデータへのアクセスにブート前認証を強制します
File Sanitizer for HP ProtectTools	• コンピューター上のデジタルのフォルダーやファイル（アプリケーション ファイル、履歴コンテンツや Web 関連コンテンツ、その他の機密データなどの機密情報）を安全にシュレッドしたり、ハードドライブ上の削除されたフォルダーやファイルを定期的にブリーチしたりします

モジュール	主要な機能
Device Access Manager for HP ProtectTools（一部のモデルのみ）	● IT 管理者が、ユーザー プロファイルに基づいてデバイスへのアクセスを制御できます ● 不正なユーザーが外部のストレージ メディアを使用してデータを削除したり、外部のメディアからシステムにウィルスを侵入させたりできないようにします ● 管理者が、特定の個人またはユーザーのグループに対して、書き込み可能なデバイスへのアクセスを無効にできます
Privacy Manager for HP ProtectTools（一部のモデルのみ）	● Microsoft の電子メールおよび Microsoft Office ドキュメントを使用するときに、通信元、通信の整合性、および通信のセキュリティを確認するために、証明機関が発行する証明書を取得するために使用されます
Computrace for HP ProtectTools（別売）	● フォルダーやファイルを安全に管理できます ● ユーザー操作や、ソフトウェアとハードウェアの変更を監視します ● ハードドライブが再フォーマットまたは交換されてもアクティブな状態を維持します ● 有効にするには、追跡契約およびトレース契約を別途購入する必要があります
Embedded Security for HP ProtectTools（一部のモデルのみ）	● TPM（Trusted Platform Module）内蔵セキュリティ チップを使用して、コンピューターに保存されているユーザー データまたは証明情報を不正なアクセスから保護します ● ユーザーのファイルおよびフォルダー情報を保護するときに役立つ PSD（Personal Secure Drive）を作成できます ● デジタル証明情報の操作を保護するための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）をサポートします

HP ProtectTools セキュリティ製品の説明と一般的な使用例

HP ProtectTools セキュリティ製品のほとんどは、パスワードを紛失したり、利用できなくなったり、忘れたりした場合、または企業のセキュリティ部門で必要となった場合にコンピューターにアクセスするためのユーザー認証機能（通常はパスワード）および管理バックアップ機能を搭載しています。

注記： 一部の HP ProtectTools セキュリティ製品は、データへのアクセスを制限するように設計されています。データの重要性が非常に高いためデータを紛失するより危険にさらすことの方が懸念される場合には、データを暗号化する必要があります。すべてのデータは安全な場所にバックアップしておくことをおすすめします。

Credential Manager for HP ProtectTools

Credential Manager（Security Manager に含まれます）は、ユーザー名とパスワードを格納します。次の用途に使用できます。

- インターネット アクセスまたは電子メールのログイン名およびパスワードを保存する
- ユーザーを Web サイトまたは電子メールに自動的にログインさせる
- 認証を管理および整理する
- Web またはネットワーク資産を選択して、リンクに直接アクセスする
- 必要に応じて名前およびパスワードを表示する

例 1：ある大規模メーカーの購買担当者は、その企業の取り引きのほとんどをインターネットで行っています。また、ログイン情報が必要となるいくつかの人気 Web サイトにもよくアクセスします。この購買担当者は、セキュリティに十分注意しているため、アカウントごとに異なるパスワードを使用しています。購買部では、Credential Manager を使用して、Web リンクごとに異なるユーザー名およびパスワードを設定することにしました。購買担当者が Web サイトのログイン画面にアクセスすると、Credential Manager によって資格情報が自動的に提供されます。ユーザー名およびパスワードが表示されるようにしたい場合は、Credential Manager で設定できます。

Credential Manager は、認証を管理および編集するためにも使用できます。ユーザーは、このツールを使用して、Web またはネットワーク資産を選択し、リンクに直接アクセスできます。また、必要に応じてユーザー名およびパスワードを表示することもできます。

例 2：ある多忙な公認会計士が、経理部全体を監督する立場に昇進しました。経理部では、多数のクライアントの Web アカウントに、それぞれ異なるログイン情報を使用してログインする必要があります。このログイン情報は複数の社員で共有する必要があるため、機密保持が問題となります。そこで、すべての Web リンク、企業ユーザー名、およびパスワードを Credential Manager for HP ProtectTools 内で整理することにしました。整理を完了させ、Credential Manager を社員に配布すれば、使用する資格情報を知らせないで社員に Web アカウントを利用させることができます。

Drive Encryption for HP ProtectTools

Drive Encryption は、コンピューターのハードドライブ全体またはセカンダリ ドライブ上にあるデータへのアクセスを制限するために使用できます。また、Drive Encryption は自己暗号化ドライブも管理できます。

例 1：ある医師が、自分のコンピューターのハードドライブにあるどのデータにも自分しかアクセスできないようにしたいと考えています。そこで、この医師は Drive Encryption を有効にし、Windows のログイン前にブート前認証が求められるようにしました。セットアップを完了すれば、オペレーティング システムの起動前にパスワードを入力しなければハードドライブにアクセスできなくなり

ます。SED（自己暗号化ドライブ）オプションでデータを暗号化するように選択すれば、ドライブのセキュリティをさらに強化することもできます。

Embedded Security for HP ProtectTools および Drive Encryption for HP ProtectTools は、どちらも暗号化したデータをコンピューターのマザーボードに関連付けるため、たとえハードディスク ドライブを取り外してもそのデータにはアクセスできません。

例 2：ある病院の経営者は、医師および承認されている人だけが、個人パスワードを共有することなく、自分たちのコンピューター内のデータにアクセスできるようにしたいと考えています。そこで、病院の IT 部門は、その経営者、医師、および承認されたすべての人を Drive Encryption ユーザーとして追加することにしました。これで、承認された人だけが個人のユーザー名およびパスワードを使用してコンピューターまたはドメインにログオンできるようになります。

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools は、インターネット ブラウザーでの行動履歴、一時ファイル、以前に削除したデータ、および他のあらゆる情報が含まれたデータを完全に削除するために使用します。File Sanitizer は、手動で実行するか、またはユーザーが定義したスケジュールに従って自動実行するように設定できます。

例 1：ある弁護士は、クライアントの機密情報を頻繁に取り扱っており、削除したファイルのデータを復元できないようにしたいと考えています。そこで、この弁護士は削除済みファイルを File Sanitizer で「シュレッド」したため、データの復元はほぼ不可能になりました。

通常、Windows でデータを削除しても、データはハードディスク ドライブから完全に消去されるわけではありません。その代わりに、Windows はハードディスク ドライブのセクターに印を付け、将来そのセクターを使用できるようにします。そのため、データが上書きされるまでは、インターネットで入手できる一般的なツールでそのデータを簡単に復元できます。File Sanitizer は、ランダムなデータをセクターに上書きするため（必要に応じて複数回実行します）、削除済みデータの読み取りや復元ができなくなります。

例 2：ある研究者は、削除済みデータ、一時ファイル、ブラウザーでの行動履歴などがログオフ時に自動でシュレッドされるようにしたいと考えています。そこで、File Sanitizer を使用して「シュレッド」のスケジュールを設定したため、一般的なファイルや独自のファイルを選択して自動的に完全消去できるようになりました。

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools は、データのコピーが可能な USB フラッシュ ドライブへの不正なアクセスをブロックするために使用できます。また、CD/DVD ドライブへのアクセス、USB デバイスの制御、ネットワーク接続などを制限することもできます。また、管理者は、ドライブへのアクセスを許可するタイミングや許可時間もスケジュール設定できます。例えば、外部の業者が社内のコンピューターにアクセスできるようにすると同時に、その業者がデータを USB ドライブにコピーできないようにする必要がある場合が考えられます。Device Access Manager for HP ProtectTools を使用すると、管理者は、ハードウェアへのアクセスを制限および管理できます。

例 1：医薬品会社のあるマネージャーは、個人の医療記録と会社のデータを仕事でよく使用しています。他の社員もこのデータにアクセスする必要がありますが、そのデータが USB デバイスや他の外部ストレージ メディアによってコンピューターからコピーされないようにすることが大変重要です。ネットワークは安全ですが、コンピューターに CD ライターや USB コネクタが搭載されているため、データがコピーされたり盗まれたりする可能性があります。そこで、このマネージャーは、Device Access Manager で CD ライターと USB コネクタを無効にし、使用できないようにしました。たとえ USB コネクタをブロックしても、マウスおよびキーボードは引き続き動作します。

例 2：ある保険会社では、社員が自宅にある個人のソフトウェアをインストールしたり、個人のデータを読み込んだりできないようにしたいと考えています。ただし、一部の社員は、すべてのコンピューターで USB コネクタにアクセスする必要があります。そこで、この会社の IT 管理者は、Device Access Manager を使用して、一部の社員に対してアクセスを許可すると同時に、その他の社員に対しては外部アクセスをブロックしました。

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools は、インターネットでの電子メールのやり取りが安全に行われるようにするために使用します。ユーザーは、認証された相手しか開くことができない電子メールを作成および送信できます。Privacy Manager を使用すると、なりすましによって情報が危険にさらされたり、傍受されたりしないようにできます。

例 1：ある証券ブローカーは、自分の電子メールが特定のクライアントだけに送信され、他の何者かが電子メール アカウントを偽装してそのメールを傍受できないようにしたいと考えています。そこで、この証券ブローカーは、Privacy Manager を使用して自分と自分のクライアントの署名を登録しました。Privacy Manager は、各ユーザーの認証証明書を（CA）をユーザーに発行します。このツールを使用すると、証券ブローカーとクライアントは、電子メールをやり取りする前に認証する必要があります。

Privacy Manager for HP ProtectTools を使用すれば、確認および認証された相手と簡単に電子メールをやり取りできるようになります。また、メール サービスを暗号化することもできます。暗号化処理は、クレジット カードを使用した一般的なオンライン ショッピングと同じように行われます。

例 2：ある CEO は、自分が電子メールで送信した情報を取締役会のメンバーだけが閲覧できるようにしたいと考えています。そこで、この CEO は、取締役とやり取りする電子メールを暗号化することにしました。Privacy Manager の認証証明書を使用すると、CEO と取締役は暗号化キーのコピーを取得し、機密性の高い電子メールを復号化できるようになります。

Computrace for HP ProtectTools（以前の LoJack Pro）

Computrace for HP ProtectTools（別売）は、盗難されたコンピューターがインターネットに接続されればいつでもその所在地を追跡できるサービスです。

例 1：ある学校の校長は、IT 部門に対し、学校にあるすべてのコンピューターを常時監視するように指示しました。そこで、学校の IT 管理者はコンピューターの保有状況を確認してから、すべてのコンピューターを Computrace に登録し、盗まれた場合に追跡できるようにしました。その後、この学校では、いくつかのコンピューターがなくなっていることに気づきました。そのため、IT 管理者は、警察に通報するとともに、Computrace の担当者に通知しました。これらのコンピューターは発見され、警察の手によって取り戻されて学校に返却されました。

Computrace for HP ProtectTools を使用すると、コンピューターをリモートで管理および特定したり、コンピューターの使用状況やアプリケーションを監視したりできます。

例 2：ある不動産会社では、世界中にあるコンピューターの管理および更新が必要になりました。そこで、Computrace を使用して、IT 担当者を実際に現地に派遣しなくてもコンピューターの監視および更新が実行できるようにしました。

Embedded Security for HP ProtectTools（一部のモデルのみ）

Embedded Security for HP ProtectTools には、Personal Secure Drive を作成できる機能が搭載されています。この機能によって、ユーザーは、アクセスするまでは完全に非表示状態となる仮想ドライブ パーティションをコンピューター上に作成できます。Embedded Security（内蔵セキュリティ）

は、他人に知られないように保護する必要があるデータと暗号化されていないデータが混在している場所で使用できます。

例 1：ある倉庫管理者はコンピューターを 1 台所有しており、複数の従業員が 1 日の間に何度かそのコンピューターにアクセスしています。管理者は、コンピューターに保存されている倉庫の機密データを暗号化し、表示されないようにしたいと考えています。また、たとえハードディスク ドライブを誰かに盗まれても、データは安全に保護され、そのデータを復号化されたり読み取られたりできないようにしたいと考えています。そこで、この倉庫管理者は、Embedded Security を有効にし、機密データを Personal Secure Drive に移動することにしました。この倉庫管理者はパスワードを入力すると、他のハードディスク ドライブとまったく同じように機密データにアクセスできます。管理者がログオフするか Personal Secure Drive を再起動すると、正しいパスワードを入力しない限りデータを表示したり開いたりできなくなります。そのため、機密データが、コンピューターを使用する他の従業員の目に触れることはありません。

Embedded Security は、マザーボードに取り付けられているハードウェア TPM（Trusted Platform Module）内の暗号化キーを保護します。これは、復号化パスワードの推測によるパスワード攻撃に対抗できる最小要件を満たした唯一の暗号化ツールです。また、Embedded Security では、ドライブ全体および電子メールも暗号化できます。

例 2：ある証券ブローカーが、ポータブル ドライブを使用して、機密度の非常に高いデータを他のコンピューターに転送しようとしてます。たとえパスワードがわかったとしても、これら 2 台のコンピューター以外ではドライブを開けないようにしたいと考えています。そこで、この証券ブローカーは、Embedded Security TPM 移行機能を使用して、データを復号化するために必要な暗号化キーをもう 1 台のコンピューターに格納できるようにしました。これによって、パスワードがわかっている場合でも、データの移動処理中にデータを復号化できるのは、この 2 台の物理コンピューターのみとなります。

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することによって、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題に対処するためのソリューションを提供できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成

盗難からの保護

盗難の例として、空港の検問所での、機密データや顧客情報を含むコンピューターの盗難が挙げられます。盗難からの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の章を参照してください。
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools モジュールで提供される Personal Secure Drive 機能では、機密データを暗号化して、認証なしではアクセスできないようにします。以下の章を参照してください。
  - Embedded Security for HP ProtectTools
- Computrace では、盗難の被害にあった後のコンピューターの場所を追跡できます。以下の章を参照してください。
  - Computrace for HP ProtectTools

機密データへのアクセス制限

契約検査官がオンサイトで作業していて、機密の財務データの確認のためにコンピューターへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報を印刷したり、ハードドライブからリムーバブル メディアにコピーしたりできないように、書き込み可能なデバイスへのアクセスを制限できます。

内部または外部からの不正なアクセスの防止

セキュリティ保護されていないコンピューターへの不正なアクセスは、金融サービス、役員、または研究開発チームからのデータなどの社内ネットワーク リソースや、患者記録や個人の財務データな

どの個人情報を非常に大きなリスクにさらすことになります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の章を参照してください。
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Password Manager は、不正なユーザーがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにするために役立ちます。
- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、書き込み可能なデバイスへのアクセスを制限できます。
- File Sanitizer を使用すると、重要なファイルやフォルダーのシュレッド、またはハードドライブ上にある削除されたフォルダーやファイルのブリーチ（以前に削除されたがハードドライブ上にはまだ存在するデータを上書きすること）によって、データを安全に削除できます。
- Privacy Manager を使用すると、Microsoft の電子メールまたは Microsoft Office ドキュメントを使用するときに、権限証明を取得できるため、重要な情報の送信と保存の処理を安全で確実なものにできます。

強力なパスワード ポリシーの作成

いくつもの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）で、パスワードやシングルサインオンのための保護されたリポジトリが提供されます。

その他のセキュリティ対策

セキュリティの役割の割り当て

コンピューターのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザーに割り当てることが重要な作業の 1 つです。

注記： 小さな組織や個人で使用する場合などは、一人の人がすべての役割を受け持つこともできます。

HP ProtectTools では、セキュリティの責任および権限を以下のように分けられます。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Drive Encryption や Embedded Security などの配備するセキュリティ機能を決定します。

  注記： HP ProtectTools の機能の多くは、セキュリティ統括責任者が HP と協力してカスタマイズできます。詳しくは、HP の Web サイト http://www.hp.com/jp/を参照してください。

- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ統括責任者がスマート カードの配備を決定した場合、IT 管理者はパスワード モードおよびスマート カード モードの両方を有効にできます。
- ユーザー：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムでスマート カードを有効にしている場合、ユーザーはスマート カードの PIN を設定し、そのカードを認証に使用できます。

注意： 管理者は、エンド ユーザーの権限の制限や、ユーザー アクセスの制限に関して「ベスト プラクティス」に従うことをおすすめします。

権限のないユーザーには管理者権限を付与しないでください。

HP ProtectTools のパスワードの管理

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）の機能のほとんどは、パスワードによってセキュリティ保護されています。以下の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者のみが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザーまたは管理者が設定できます。

HP ProtectTools のパスワード	設定するモジュール	機能
Windows のログオン パスワード	Windows の[コントロール パネル]または HP ProtectTools Security Manager	HP ProtectTools Security Manager のさまざまな機能にアクセスするための手動ログオンまたは認証に使用できます
HP ProtectTools Security Manager の[バックアップおよび復元]パスワード	HP ProtectTools Security Manager（ユーザーごと）	HP ProtectTools Security Manager の[バックアップおよび復元]ファイルへのアクセスを保護します

HP ProtectTools のパスワード	設定するモジュール	機能
スマート カードの PIN	Credential Manager	マルチファクター認証として使用できます Windows 認証として使用できます スマート カード トークンが選択されている場合は、Drive Encryption のユーザーを認証します
緊急リカバリ トークンのパスワード	Embedded Security、IT 管理者が設定	内蔵セキュリティ チップ用のバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します
所有者のパスワード	Embedded Security、IT 管理者が設定	システムと TPM チップを、Embedded Security のすべての所有者機能への不正なアクセスから保護します
BIOS 管理者パスワード	[Computer Setup]、IT 管理者が設定	[Computer Setup]ユーティリティへのアクセスを保護します

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成し、そのパスワードが危険にさらされないようにするために、以下のガイドラインを参考にしてください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は、常に半角アルファベットと半角数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの l または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分けます。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字をその次の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピューターのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピューター上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

HP ProtectTools 証明情報のバックアップおよび復元

HP ProtectTools の[バックアップおよび復元]機能を使用して、HP ProtectTools 証明情報のデータおよび設定を選択したりバックアップしたりできます。

2　セットアップ ウィザードをお使いになる前に

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）セットアップ ウィザードでは、このコンピューターのすべてのユーザーに適用される使用可能なセキュリティ機能を有効にします。管理者コンソールの[Security Features]（セキュリティ機能）ページでこれらの機能を管理することもできます。

HP ProtectTools Security Manager セットアップ ウィザードからセキュリティ機能をセットアップするには、以下の操作を行います。

1. Windows サイドバーにある[HP ProtectTools]デスクトップ ガジェット アイコンまたはタスク バーの右端の通知領域にあるタスク バー アイコンから HP ProtectTools Security Manager を起動します。

   [HP ProtectTools]デスクトップ ガジェット アイコンのバナーの色は、以下のどれかの状況を示しています。

   - 赤色：HP ProtectTools がセットアップされていないか、または HP ProtectTools モジュールのどれかがエラー状態になっています。
   - 黄色：HP ProtectTools Security Manager の[アプリケーションの状態]ページで、変更が必要な設定がないかどうか確認してください。
   - 青色：HP ProtectTools はセットアップされ、正しく動作しています。

以下のどれかの状況を示すメッセージがガジェット アイコンの下部に表示されます。

- **[今すぐセットアップ]**：管理者はガジェット アイコンをクリックして Security Manager のセットアップ ウィザードを実行し、コンピューターの認証資格情報を設定する必要があります。

  セットアップ ウィザードは独立したアプリケーションです。

- **[今すぐ登録]**：ユーザーはガジェット アイコンをクリックして Security Manager の[使用開始準備]ウィザードを実行し、認証資格情報を登録する必要があります。

  [使用開始準備]ウィザードが[HP ProtectTools Security Manager]ダッシュボードに表示されます。

- **[今すぐチェック]**：ガジェット アイコンをクリックして、[セキュリティ アプリケーションの状態]ページに詳細を表示します。

注記： [HP ProtectTools]デスクトップ ガジェット アイコンは、Windows XP では使用できません。

または

[スタート]→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。左側の枠内で、**[セットアップ ウィザード]**をクリックします。

2. [ようこそ]画面の内容を確認して、**[次へ]**をクリックします。

3. Windows パスワードを入力してユーザー情報を認証し、**[次へ]**をクリックします。

   Windows パスワードをまだ作成していない場合は、作成するよう求められます。お使いの Windows アカウントが第三者から不正にアクセスされないようにするために、また HP ProtectTools Security Manager の機能を使用するためには、Windows パスワードが必要となります。

4. [SpareKey]ページで、3 つのセキュリティに関する質問を選択し、各質問の回答を入力してから、**[次へ]**をクリックします。

   [HP ProtectTools Security Manager]ダッシュボード内の**[Credential Manager]**の[SpareKey]ページで、別の質問を選択したり、回答を変更したりできます。

   注記： この HP SpareKey のセットアップは、管理者権限のあるユーザーにのみ適用されます。

5. チェック ボックスにチェックを入れてセキュリティ機能を有効にし、**[次へ]**をクリックします。

   選択する機能が多いほど、コンピューターのセキュリティは高くなります。

   注記： これらの設定はすべてのユーザーに適用されます。すべてのチェック ボックスにチェックが入っていない場合、セットアップ ウィザードでは証明情報の登録を求めるメッセージを表示しません。

   - **[Windows へのログオンの保護]**：アクセスのために特定の証明情報を使用するよう求めることで、Windows アカウントを保護できます。

   - **[ドライブの暗号化機能]**：ハードドライブを暗号化して、適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護できます。

   - **[ブート前セキュリティ機能]**：Windows の起動前に、不正なユーザーによるアクセスを禁止することによってコンピューターを保護できます。

注記： BIOS によってサポートされていない場合は、[ブート前セキュリティ]を使用できません。

6. セットアップ ウィザードでは証明情報を登録するよう求められます。

   指紋認証システム、スマート カード、Web カメラのどれも使用できない場合は、Windows パスワードを入力するよう求められます。登録後は、認証が必要になった場合はいつでも登録した認証情報を使用できます。

   注記： これらの証明情報の登録は、管理者権限のあるユーザーにのみ適用されます。

7. ウィザードの最後のページで、[**完了**]をクリックします。

   [HP ProtectTools Security Manager]ダッシュボードの[ホーム]ページが表示されます。

3 HP ProtectTools Security Manager 管理者コンソール

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）ソフトウェアには、コンピューター、ネットワーク、および重要なデータに対する不正アクセスの防止に役立つセキュリティ機能があります。HP ProtectTools Security Manager の管理は、管理者コンソールの機能を通して提供されます。

また、[HP ProtectTools Security Manager]ダッシュボードでは、コンピューターを紛失したり盗難されたりした場合にその回復に役立てることができる、追加のアプリケーションを利用できます（一部のモデルのみ）。

コンソールを使用すると、ローカルの管理者は以下のタスクを実行できます。

- セキュリティ機能の有効化または無効化
- 認証に必要な証明情報の指定
- コンピューターのユーザーの管理
- デバイス固有のパラメーターの調整
- インストールされている HP ProtectTools Security Manager アプリケーションの設定
- HP ProtectTools Security Manager アプリケーションの追加

HP ProtectTools 管理者コンソールを開く

システム ポリシーの設定やソフトウェアの設定などの管理タスクを行う場合は、以下の操作を行ってコンソールを開きます。

▲ [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。

　または

　HP ProtectTools Security Manager の左側の枠内で、[**管理**]→[**管理者コンソール**]の順にクリックします。

管理者コンソールの使用

HP ProtectTools 管理者コンソールは、HP ProtectTools Security Manager の機能およびアプリケーションを管理するための中心となる場所です。

▲ HP ProtectTools 管理者コンソールを開くには、[**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。

または

HP ProtectTools Security Manager の左側の枠内で、[**管理**]→[**管理者コンソール**]の順にクリックします。

このコンソールは、以下のコンポーネントで構成されています。

- [**ホーム**]：次のセキュリティ オプションを設定できます。
  - [**システム セキュリティの強化**]
  - [**強力な認証を求める**]
  - [**HP ProtectTools ユーザーの管理**]
  - [**HP ProtectTools を集中管理する方法を参照してください**]
- [**システム**]：ユーザーやデバイスの次のセキュリティ機能および認証を設定できます。
  - [**セキュリティ**]
  - [**ユーザー**]
  - [**証明情報**]
- [**アプリケーション**]：HP ProtectTools Security Manager および HP ProtectTools Security Manager アプリケーションの設定を設定できます。
- [**データ**]：データを保護する HP ProtectTools Security Manager アプリケーションへのリンクの展開メニューを提供します。
- [**Central Management**]（集中管理）：追加のソリューション、製品アップデート、およびメッセージにアクセスするためのタブが表示されます。
- [**セットアップ ウィザード**]：HP ProtectTools Security Manager を設定できます。
- [**バージョン情報**]：バージョン番号や著作権情報などの、HP ProtectTools Security Manager に関する情報を表示します。
- [**メイン領域**]：アプリケーション固有の画面を表示します。

  [**?**]：管理者コンソール ソフトウェアのヘルプが表示されます。このアイコンはウィンドウ枠の右上の最小化アイコンおよび最大化アイコンの隣にあります。

システムの設定

[**システム**]グループには、HP ProtectTools 管理者コンソールの画面の左側にあるメニュー パネルからアクセスします。このグループ内のアプリケーションを使用して、コンピューター、ユーザー、およびデバイスのポリシーや設定を管理できます。

[**システム**]グループには、以下のアプリケーションが含まれています。

- [**セキュリティ**]：このコンピューターに対する、ユーザーの対話操作の方法を管理する機能、認証、および設定を管理します。
- [**ユーザー**]：このコンピューターのユーザーを設定、管理、および登録します。
- [**証明情報**]：コンピューターに内蔵または接続されているセキュリティ デバイスの設定を管理します。

コンピューターでの認証の設定

認証アプリケーション内で、コンピューターへのアクセスを管理するポリシーを設定できます。Windows にログオンするとき、またはユーザー セッション中に Web サイトやプログラムにログオンするときに各クラスのユーザーを認証するために必要な証明情報を指定できます。

コンピューターでの認証を設定するには、以下の操作を行います。

1. 管理者コンソールの左側の枠内で、[**セキュリティ**]をクリックしてから[**認証**]をクリックします。
2. ログオン認証を設定するには、[**ログオン ポリシー**]タブをクリックし、変更を行ってから[**適用**]をクリックします。
3. セッション認証を設定するには、[**セッション ポリシー**]タブをクリックし、変更を行ってから[**適用**]をクリックします。

ログオン ポリシー

Windows にログオンするときにユーザーを認証するために必要な証明情報を管理するポリシーを定義するには、以下の操作を行います。

1. 管理者コンソールの左側の枠内で、[**セキュリティ**]をクリックしてから[**認証**]をクリックします。
2. [**ログオン ポリシー**]タブで、下向き矢印をクリックしてからユーザーのカテゴリをクリックします。
   - [**このコンピューターの管理者の場合**]
   - [**管理者以外のユーザーの場合**]
3. 選択したユーザーのカテゴリに必要な認証証明情報を指定します。
4. ユーザーを認証するために、指定した証明情報のどれか 1 つが必要なのか、または指定した証明情報のすべてが必要なのかを選択します。
5. [**適用**]をクリックします。

セッション ポリシー

Windows セッション中に HP ProtectTools アプリケーションにアクセスするために必要な証明情報を管理するポリシーを定義するには、以下の操作を行います。

1. 管理者コンソールの左側の枠内で、[**セキュリティ**]をクリックしてから[**認証**]をクリックします。
2. [**セッション ポリシー**]タブで、下向き矢印をクリックしてからユーザーのカテゴリをクリックします。
   - [**このコンピューターの管理者の場合**]
   - [**管理者以外のユーザーの場合**]
3. 下向き矢印をクリックしてから、選択したユーザーのカテゴリに必要な認証証明情報を指定します。
   - [**指定された資格情報のうちの 1 つを要求する**]

     注記： すべての資格情報のチェック ボックスのチェックを外すと、[**認証を要求しない**]を選択した場合と同じ設定になります。

   - [**指定されたすべての資格情報を要求する**]
   - [**認証を要求しない**]：このオプションを選択すると、すべての証明情報がウィンドウから消去されます。
4. [**適用**]をクリックします。

設定

1. 以下の設定を有効にするにはチェック ボックスにチェックを入れ、無効にするにはチェック ボックスのチェックを外します。

   [**ワン ステップ ログオンを許可する**]：BIOS または暗号化されたディスクのレベルで認証が実行された場合は、このコンピューターのユーザーが Windows のログオンを省略できるようにします。
2. [**適用**]をクリックします。

ユーザーの管理

ユーザー アプリケーション内で、このコンピューターの HP ProtectTools ユーザーを監視したり管理したりできます。

すべての HP ProtectTools ユーザーが一覧表示され、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を使用して設定されたポリシーに対して検証されます。一覧表示および検証は、これらのユーザーが各ポリシーを満たすことができる適切な証明情報を登録しているかどうかに関係なく行われます。

ユーザーを管理するには、以下の設定のどれかを選択します。

- ユーザーを追加するには、[**追加**]をクリックします。
- ユーザーを削除するには、そのユーザーをクリックしてから[**削除**]をクリックします。

- ユーザーの追加の証明情報を設定するには、そのユーザーをクリックしてから、[**登録**]をクリックします。
- 特定のユーザーのポリシーを確認するには、そのユーザーを選択してからウィンドウ下部のポリシーを確認します。

証明情報

証明情報アプリケーション内で、HP ProtectTools Security Manager によって認識される内蔵デバイスまたは接続されているセキュリティ デバイスで使用できる設定を指定できます。

SpareKey

Windows ログオンでの HP SpareKey 認証を許可するかどうかを設定し、SpareKey 登録時にユーザーに表示されるセキュリティに関する質問を管理できます。

1. Windows ログオンでの HP SpareKey 認証の使用を有効にするにはチェック ボックスにチェックを入れ、無効にするにはチェック ボックスのチェックを外します。
2. HP SpareKey の登録中にユーザーに表示されるセキュリティに関する質問を選択します。最大 3 つの質問をユーザー自身で作成して指定したり、ユーザーが独自のパスフレーズを入力できるようにしたりできます。
3. [**適用**]をクリックします。

指紋

コンピューターに指紋認証システムがインストールまたは接続されている場合、[指紋]ページに以下のタブが表示されます。

- [**登録**]：ユーザーが登録できる指紋の最小数と最大数を選択できます。

  また、指紋認証システムからすべてのデータをクリアすることもできます。

  注意： 指紋認証システムのすべてのデータをクリアすると、管理者を含む、すべてのユーザーの指紋データが消去されます。ログオン ポリシーで指紋のみを求めるようにしている場合は、すべてのユーザーがコンピューターにログオンできなくなることがあります。

- [**感度**]：指紋が読み取られるときに指紋認証システムで使用される感度を調整するには、スライダーを移動します。

  指紋が常に認識されない場合は、より低い感度を選択することが必要な場合があります。この設定を高くすると指紋の読み取りの変化に対する感度が向上するため、誤って受け入れられる可能性が減ります。[**中-高**]に設定すると、セキュリティおよび利便性の適切な組み合わせが得られます。

- [**詳細設定**]：以下のオプションのどれかを選択して、節電し、視覚的情報を向上するように指紋認証システムを設定します。
  - [**最適化**]：指紋認証システムは、必要に応じて有効になります。指紋認証システムが最初に使用されるときに、わずかな遅延が発生する場合があります。
  - [**節電**]：指紋認証システムは応答が遅くなりますが、必要な電力は少なくなります。
  - [**通常の電力**]：指紋認証システムは常に使用できる状態ですが、この設定は電力を最も多く使用します。

スマート カード

コンピューターにスマート カード リーダーがインストールまたは接続されている場合、[スマート カード]ページに 2 つのタブが表示されます。

- **[設定]**：スマート カードが取り外されたときは、自動的にロックするようにコンピューターを設定します。

注記：　コンピューターがロックするのは、そのスマート カードが Windows へのログオン時の認証証明情報として使用されていた場合のみです。Windows へのログオンに使用されていなかったスマート カードを取り外しても、コンピューターはロックされません。

- **[管理]**：以下のオプションから選択します。
  - **[スマート カードの初期化]**：HP Protect Tools で使用するためにスマート カードを準備します。HP ProtectTools 以外で初期化され、非対称のキーペアと関連する証明書を含んでいるスマート カードを使用する場合は、特定の証明書による初期化が必要でない限り、再度初期化する必要はありません。
  - **[スマート カードの暗証番号の変更]**：スマート カードで使用する PIN を変更できます。
  - **[HP ProtectTools データのみを消去]**：カードの初期化中に作成される HP ProtectTools 証明書のみを消去します。その他のデータはカードから消去されません。
  - **[スマート カードのすべてのデータの消去]**：指定されたスマート カードのすべてのデータを消去します。カードは、HP ProtectTools またはその他のアプリケーションで使用できなくなります。

注記：　スマート カードによってサポートされていない機能は使用できません。

▲ **[適用]**をクリックします。

顔

コンピューターに Web カメラがインストールまたは接続されていて、Face Recognition プログラムがインストールされている場合、コンピューターの使い勝手とセキュリティが侵害される危険性の低さとの間でバランスを取るように Face Recognition のセキュリティ レベルを設定できます。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. **[資格情報]**→**[顔]**の順にクリックします。
3. 利便性を高めるには、スライダーをクリックして左にスライドさせ、精度を高めるには、スライダーをクリックして右にスライドさせます。
   - **[利便性]**：登録したユーザーが、条件がよくない場合でも簡単にアクセスできるようにするには、スライダーのバーをクリックしてスライダーを**[利便性]**の位置まで動かします。
   - **[バランス]**：セキュリティと使い勝手を適度に両立させる場合、機密情報がある場合、または不正なログインを試みられる可能性がある場所にコンピューターがある場合には、スライダーのバーをクリックしてスライダーを**[バランス]**の位置まで動かします。
   - **[精度]**：登録したシーンまたは現在の照明の状態が通常よりも悪いときに、ユーザーをアクセスしづらくして、ユーザーが誤って受け入れられてしまう可能性を低くする場合には、スライダーのバーをクリックしてスライダーを**[精度]**の位置に移動します。

4. [**詳細設定**]をクリックし、追加のセキュリティを設定します。詳しくは、42 ページの「詳細ユーザー設定」を参照してください。

5. [**適用**]をクリックします。

アプリケーションの設定

[設定]を使用して、現在インストールされている HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）アプリケーションの動作をカスタマイズできます。

アプリケーションの設定を編集するには、以下の操作を行います。

1. 管理者コンソールの左側の枠内の[**アプリケーション**]で、[**設定**]をクリックします。
2. 特定の設定を有効にするには隣にあるチェック ボックスにチェックを入れ、設定を無効にするにはチェック ボックスのチェックを外します。
3. [**適用**]をクリックします。

[全般]タブ

[**全般**]タブでは、以下の設定を使用できます。

- [**管理者用のセットアップ ウィザードを自動的に起動しない**]：ログオン時にウィザードが自動的に開かないようにするには、このオプションを選択します。
- [**ユーザー用の使用開始準備ウィザードを自動的に起動しない**]：ログオン時にユーザーの設定が自動的に開かないようにするには、このオプションを選択します。

[アプリケーション]タブ

ここに表示される設定は、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）に新しいアプリケーションが追加されると変更される可能性があります。初期設定で表示される最小限の設定は、以下のとおりです。

- [**アプリケーションの状態**]：すべてのアプリケーションに対する状態の表示を有効にします。
- [**パスワード マネージャー**]：コンピューターのすべてのユーザーに対して Password Manager を有効にします。
- [**Privacy Manager**]：コンピューターのすべてのユーザーに対して Privacy Manager を有効にします。
- [**Enable the Central Management link**]（[集中管理]リンクを有効にする）：このコンピューターのすべてのユーザーが[**Central Management**]（集中管理）をクリックすることによって HP ProtectTools Security Manager にアプリケーションを追加できるようにします。

すべてのアプリケーションを工場出荷時の設定に戻すには、[**初期設定に設定**]ボタンをクリックします。

Central Management（集中管理）

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）では、新しい管理ツールを追加するために、追加のアプリケーションを使用できます。このコンピューターの管理者

は、[設定]ページでこの機能を無効にできます。[Central Management]ページには、2 つのタブがあります。

- **[ビジネス ソリューション]**：インターネット接続が利用できる場合は、DigitalPersona の Web サイト（http://www.digitalpersona.com/）（英語サイト）にアクセスして、新しいアプリケーションを確認できます。
- **[更新およびメッセージ]**
    - 新しいアプリケーションおよび更新についての情報を要求するには、**[新しいアプリケーションおよび更新に関する通知を受け取る]**チェック ボックスにチェックを入れます。
    - 自動更新のスケジュールを設定するには、その間隔となる日数を選択します。
    - 更新を確認するには、**[今すぐチェック]**をクリックします。

4 HP ProtectTools Security Manager

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を使用すると、お使いのコンピューターのセキュリティを大幅に強化できます。

プリロードされている HP ProtectTools Security Manager の各アプリケーション、および Web からいつでもダウンロードできる追加アプリケーションを使用して、以下のタスクを実行できます。

- ログオンおよびパスワードを管理する
- Windows オペレーティング システムのパスワードを簡単に変更する
- プログラムのオプションを設定する
- 指紋を利用してセキュリティと利便性を強化する
- 認証用のシーンを 1 つ以上登録する
- 認証用のスマート カードをセットアップする
- プログラムのバックアップおよび復元を実行する
- アプリケーションをさらに追加する

Security Manager（セキュリティ マネージャー）を開く

以下のどれかの方法で Security Manager を開きます。

- ［**スタート**］→［**すべてのプログラム**］→［**HP**］→［**HP ProtectTools Security Manager**］の順にクリックします。
- タスクバーの右端の通知領域にある［**HP ProtectTools**］アイコンをダブルクリックします。
- ［**HP ProtectTools**］アイコンを右クリックして、［**HP ProtectTools Security Manager を開く**］をクリックします。
- ［**HP ProtectTools**］デスクトップ ガジェット アイコンをクリックします。
- ctrl ＋ Windows ロゴ キー＋ h ホットキーを使用して、HP ProtectTools Security Manager の［**クイック リンク**］メニューを開きます。

  ホットキーの変更について詳しくは、36 ページの「設定」を参照してください。

Security Manager のダッシュボードの使用

[HP ProtectTools Security Manager]ダッシュボードは、HP ProtectTools Security Manager の機能、アプリケーション、および設定に簡単にアクセスするための中心となる場所です。

▲ [HP ProtectTools Security Manager]ダッシュボードを開くには、**[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。

ダッシュボードには以下のコンポーネントが表示されます。

- **[ID カード]**：ログオン中のユーザー アカウントを識別する、Windows ユーザー名および選択済みの画像を表示します。
- **[セキュリティ アプリケーション]**：以下のカテゴリのセキュリティを設定できる、リンクの展開メニューを提供します。
  - **[ホーム]**：パスワードを管理したり、認証資格情報をセットアップしたり、セキュリティ アプリケーションの状態を確認したりします。
  - **[状態]**：HP ProtectTools セキュリティ アプリケーションの状態を確認します。

注記： 以下のうち、コンピューターにインストールされていないアプリケーションは表示されません。

- **[マイ ログオン]**：パスワード マネージャー、Credential Manager、パスワード、HP SpareKey、スマート カード、顔認証、および指紋によって認証資格情報を管理します。
- **[マイ データ]**：Drive Encryption および File Sanitizer によってデータのセキュリティを管理します。
- **[マイ コンピューター]**：Device Access Manager によってコンピューターのセキュリティを管理します。
- **[マイ通信]**：Privacy Manager によって通信のセキュリティを管理します。
- **[管理]**：管理者は以下のオプションにアクセスできます。
  - **[管理者コンソール]**：管理者はセキュリティおよびユーザーを管理できます。
  - **[Central Management]**（集中管理）：管理者は追加のソリューション、製品アップデート、およびメッセージにアクセスできます。
- **[詳細設定]**：以下のような追加機能にアクセスするためのコマンドが表示されます。
  - **[設定]**：HP ProtectTools Security Manager の個人設定を実行できます。
  - **[バックアップおよび復元]**：データをバックアップまたは復元できます。
  - **[バージョン情報]**：バージョン番号や著作権情報などの、HP ProtectTools Security Manager に関する情報を表示します。
- **[メイン領域]**：アプリケーション固有の画面を表示します。
- **[?]**：Security Manager ソフトウェアのヘルプを表示します。このアイコンはウィンドウの右上の最小化アイコンおよび最大化アイコンの隣にあります。

セキュリティ アプリケーションの状態

インストールされているセキュリティ アプリケーションの状態は、2 つの場所で確認できます。

- **[[HP ProtectTools]デスクトップ ガジェット]**

  [HP ProtectTools]ガジェット アイコンの上部のバナーの色が、インストールされたセキュリティ アプリケーションの全体的なセキュリティ状態を反映するように変化します。

  ◦ 赤色：警告

  ◦ 黄色：注意：設定されていません

  ◦ 青色：OK

  以下のどれかの状況を示すメッセージがガジェット アイコンの下部に表示されます。

  ◦ **[今すぐセットアップ]**：管理者はガジェット アイコンをクリックして Security Manager のセットアップ ウィザードを実行し、コンピューターの認証資格情報を設定する必要があります。

    セットアップ ウィザードは独立したアプリケーションです。

  ◦ **[今すぐ登録]**：ユーザーはガジェット アイコンをクリックして Security Manager の[使用開始準備]ウィザードを実行し、認証資格情報を登録する必要があります。

    [使用開始準備]ウィザードが[HP ProtectTools Security Manager]ダッシュボードに表示されます。

  ◦ **[今すぐチェック]**：ガジェット アイコンをクリックして、[セキュリティ アプリケーションの状態]ページに詳細を表示します。

- **[セキュリティ アプリケーションの状態]**ページ：[HP ProtectTools Security Manager]ダッシュボードの**[状態]**をクリックして、インストールされたセキュリティ アプリケーションの全体的な状態および各アプリケーションの状態を表示します。

マイ ログオン

このグループに含まれるアプリケーションによって、ユーザーのデジタル ID をさまざまな面から管理できます。

- ［**パスワード マネージャー**］：クイック リンクを作成および管理します。クイック リンクを使用すると、Windows パスワード、指紋、またはスマート カードによる認証を行うことで、Web サイトおよびプログラムを起動し、ログオンできます。
- ［**Credential Manager**］：Windows パスワードの変更、指紋の登録、またはスマート カードのセットアップを簡単に実行できるようにします。

管理者は、ダッシュボードの左下隅にある［**管理**］→［**Central Management**］（集中管理）の順にクリックして、アプリケーションをさらに追加できます。

パスワード マネージャー

パスワード マネージャーを使用すると、Windows、Web サイト、およびアプリケーションへのログオンがより簡単かつ安全になります。パスワード マネージャーによって、書き留めたり覚えたりする必要がなく強固なパスワードを作成できるため、指紋、スマート カード、または Windows パスワードを使用してすばやく簡単にログオンできるようになります。

パスワード マネージャーには以下のオプションがあります。

- ［**管理**］タブでログオンを追加、編集、または削除する。
- クイック リンクを使用して初期設定のブラウザーを起動し、セットアップ済みの Web サイトまたはプログラムにログオンする。
- ドラッグ アンド ドロップ操作でクイック リンクをカテゴリ別に整理する。
- セキュリティ上のリスクがあるパスワードをすぐに見つけ出し、複雑で強固なパスワードを自動生成して新しいサイトで利用できるようにする。

［**パスワード マネージャー**］アイコンは、Web ページまたはアプリケーションのログオン画面の左上隅に表示されます。Web サイトまたはアプリケーション用のログオン情報が作成されていない場合は、プラス記号（＋）がアイコン上に表示されます。

▲ ［**パスワード マネージャー**］アイコンをクリックしてコンテキスト メニューを表示すると、以下のオプションを選択できます。

ログオン情報が作成されていない Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- ［**[パスワード マネージャー]への[任意のドメイン]の追加**］：表示中のログオン画面用にログオンを追加できます。
- ［**[パスワード マネージャー]を開く**］：パスワード マネージャーを起動します。
- ［**アイコンの設定**］：［**パスワード マネージャー**］アイコンを表示する条件を指定できます。
- ［**ヘルプ**］：Security Manager ソフトウェアのヘルプを表示します。

ログオン情報が作成されている Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- ［**ログオン データの入力**］: ログオン データをログオン用フィールドに入力してページを送信します（ログオンを作成または最後に編集したときに送信を指定していた場合）。
- ［**ログオンの編集**］: 表示中の Web サイト用のログオン データを編集できます。
- ［**ログオンの追加**］: アカウントをログオンに追加できます。
- ［**[パスワード マネージャー]を開く**］: パスワード マネージャーを起動します。
- ［**ヘルプ**］: Security Manager ソフトウェアのヘルプを表示します。

注記： HP ProtectTools Security Manager は、証明情報を確認するときに、複数の証明情報が求められるようにコンピューターの管理者によってセットアップされていることがあります。

ログオン情報の追加

Web サイトまたはプログラム用のログオンは、ログオン情報を 1 回入力すれば、簡単に追加できます。以降は、パスワード マネージャーによって情報が自動的に入力されるようになります。これらのログオンは、その Web サイトまたはプログラムを表示すると使用できるようになります。また、［**ログオン**］メニューからログオンをクリックし、パスワード マネージャーでその Web サイトまたはプログラムを表示させてログオンすることもできます。

ログオン情報を追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. ［**パスワード マネージャー**］アイコンの矢印をクリックし、ログオン画面の種類（Web サイト用またはプログラム用）に応じて以下のどちらかをクリックします。
   - Web サイトの場合は、［**[パスワード マネージャー]への[任意のドメイン]の追加**］をクリックします。
   - プログラムの場合は、［**[パスワード マネージャー]へのログオンの追加**］をクリックします。
3. ログオン データを入力します。画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。［**Password Manager Manage**］（パスワード マネージャーの管理）タブから［**ログオンの追加**］をクリックして、このダイアログ ボックスを表示させることもできます。ctrl ＋ Windows ロゴ キー＋ h ホットキーの使用や指紋の読み取り、またスマート カードの挿入など、コンピューターに接続されているセキュリティ デバイスに依存するオプションもあります。
   a. あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。
   b. このログオン用のパスワードを表示するには、［**パスワードを表示する**］をクリックします。
   c. ログオン用フィールドの入力後に送信を実行しない場合は、［**ログオン データを自動的に送信する**］チェック ボックスのチェックを外します。
   d. VeriSign VIP セキュリティを有効にするには、［**I want VIP security on this site**］（このサイトで VIP セキュリティを使用する）チェック ボックスにチェックを入れます。

このオプションは、VeriSign Identity Protection（VIP）が使用可能なサイトに対してのみ表示されます。サイトでサポートされている場合は、通常の認証方法と共に VIP セキュリティ コードが自動的に入力されるように選択することもできます。

e. [**OK**]をクリックし、使用する認証方法（指紋、パスワード、または顔認証）をクリックし、選択した認証方法を使用してログオンします。

[**パスワード マネージャー**]アイコンのプラス記号（＋）が消え、ログオン情報が作成されたことが示されます。

f. パスワード マネージャーでログオン用フィールドが検出されない場合は、[**その他のフィールド**]をクリックします。

- ログオンに必要な各フィールドのチェック ボックスにチェックを入れ、ログオンに不要なフィールドのチェック ボックスのチェックを外します。
- パスワード マネージャーで検出できないログオン用フィールドがある場合は、続行するかどうかを確認するメッセージが表示されます。[**はい**]をクリックします。
- ログオン用フィールドにデータが入力された状態でダイアログ ボックスが開きます。各フィールドのアイコンをクリックし、該当するログオン用フィールドにドラッグしてから、ボタンをクリックして Web サイトにサインインします。

注記： 特定のサイトでログオン データの入力に手動モードを使用した場合は、以後その Web サイトにログオンするときに、常にこの方法を使用する必要があります。

注記： ログオン データの手動入力モードを使用できるのは、Internet Explorer 8 のみです。

- [**閉じる**]をクリックします。

この Web サイトまたはプログラムにアクセスすると、そのたびに Web サイトまたはアプリケーションのログオン画面の左上隅に[**パスワード マネージャー**]アイコンが表示され、登録済みの証明情報を使用してログオンできることが示されます。

ログオンの編集

ログオンを編集するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. ログオン情報を編集できるダイアログ ボックスを表示するには、[**パスワード マネージャー**]アイコンの矢印→[**ログオンの編集**]の順にクリックします。画面のログオン用フィールドおよびダイアログ ボックスの対応するフィールドが、オレンジ色の太い枠線で識別されます。

   [**Password Manager Manage**]（パスワード マネージャーの管理）タブから[**目的のログオンの編集**]をクリックして、このダイアログ ボックスを表示させることもできます。
3. ログオン情報を編集します。
   - [**ユーザー名**]ログオン フィールドであらかじめフォーマットが用意された選択肢の 1 つを選択するには、フィールドの右側にある矢印をクリックします。
   - [**パスワード**]ログオン フィールドであらかじめフォーマットが用意された選択肢の 1 つを選択するには、フィールドの右側にある矢印をクリックします。
   - VeriSign VIP セキュリティを有効にするには、[**I want VIP security on this site**]（このサイトで VIP セキュリティを使用する）チェック ボックスにチェックを入れます。

このオプションは、VeriSign VIP セキュリティが使用可能なサイトに対してのみ表示されます。サイトでサポートされている場合は、通常の認証方法と共に VIP セキュリティ コードが自動的に入力されるように選択することもできます。

- 画面上の他のフィールドをログオンに追加するには、[**その他のフィールド**]をクリックします。
- このログオン用のパスワードを表示するには、[**パスワードを表示する**]をクリックします。
- ログオン用フィールドの入力後に送信を実行しない場合は、[**ログオン データを自動的に送信する**]チェック ボックスのチェックを外します。

4. [**OK**]をクリックします。

ログオン メニューの使用

パスワード マネージャーでは、ログオンを作成した Web サイトおよびプログラムをすばやく簡単に起動できます。[**ログオン**]メニューまたはパスワード マネージャーの[**管理**]タブからプログラムまたは Web サイトをダブルクリックし、ログオン画面を表示して、ログオン データを入力します。

作成したログオンは、パスワード マネージャーの[**ログオン**]メニューに自動的に追加されます。

[**ログオン**]メニューを表示するには、以下の操作を行います。

1. [**パスワード マネージャー**]のホットキー（ctrl ＋ Windows ロゴ キー＋ h が工場出荷時の設定です）を押します。ホットキーを変更するには、[HP ProtectTools Security Manager]ダッシュボードで[**パスワード マネージャー**]→[**設定**]の順にクリックします。
2. （指紋認証システムが内蔵または接続されたコンピューターで）指を滑らせて指紋を読み取らせるか、Windows パスワードを入力します。

ログオンをカテゴリ別に整理

ログオンを整理するには、1 つ以上のカテゴリを作成します。その後、ログオンを目的のカテゴリにドラッグ アンド ドロップします。

カテゴリを追加するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードで、[**パスワード マネージャー**]をクリックします。
2. [**管理**]タブ→[**カテゴリの追加**]の順にクリックします。
3. カテゴリの名前を入力します。
4. [**OK**]をクリックします。

ログオンをカテゴリに追加するには、以下の操作を行います。

1. マウス ポインターを目的のログオンの上に置きます。
2. マウスの左ボタンを押したままにします。
3. ログオンをカテゴリの一覧にドラッグします。マウス ポインターをカテゴリの上に置くと、そのカテゴリが強調表示されます。
4. 目的のカテゴリが強調表示されたら、マウス ボタンを放します。

ログオンは、選択したカテゴリに移動されるのではなく、コピーされるのみです。そのため、同じログオンを複数のカテゴリに追加できます。[**すべて**]をクリックするとすべてのログオンを表示できます。

ログオンの管理

パスワード マネージャーを使用すると、ユーザー名、パスワード、および複数のログオン アカウントのログオン情報を、中心となる 1 つの場所から簡単に管理できます。

ログオン情報は[**管理**]タブに一覧表示されます。同じ Web サイトに対して複数のログオン情報が作成されている場合、各ログオンはその Web サイト名の下に一覧表示され、ログオン一覧の中でインデント表示されます。

ログオンを管理するには、以下の操作を行います。

▲ [HP ProtectTools Security Manager]ダッシュボードで、[**パスワード マネージャー**]→[**管理**]タブの順にクリックします。

- [**ログオンの追加**]:[**ログオンの追加**]をクリックし、画面の説明に沿って操作します。
- [**ログオン**]:既存のログオンをクリックし、以下のオプションのどれかを選択し、画面の説明に沿って操作します。
    - [**開く**]:既存のログオンがある Web サイトまたはプログラムを開きます。
    - [**追加**]:ログオンを追加します。詳しくは、31 ページの「ログオン情報の追加」を参照してください。
    - [**編集**]:ログオンを編集します。詳しくは、32 ページの「ログオンの編集」を参照してください。
    - [**削除**]:既存のログオンがある Web サイトまたはプログラムを削除します。
- [**カテゴリの追加**]:[**カテゴリの追加**]をクリックし、画面の説明に沿って操作します。詳しくは、33 ページの「ログオンをカテゴリ別に整理」を参照してください。

Web サイトまたはプログラムに他のログオンを追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [**パスワード マネージャー**]アイコンをクリックして、コンテキスト メニューを表示します。
3. [**ログオンの追加**]をクリックし、画面の説明に沿って操作します。

パスワード強度の評価

証明情報を保護するには、Web サイトおよびプログラムに強固なパスワードを使用することが重要です。

パスワード マネージャーでは、Web サイトおよびプログラムへのログオンに使用されている各パスワードの強度を自動的にすばやく分析することで、セキュリティを監視および強化できます。

[パスワード マネージャー]アイコンの設定

パスワード マネージャーは、Web サイトおよびプログラムのログオン画面を識別します。ログオン情報が作成されていないログオン画面が検出されると、パスワード マネージャーによってプラス記

号（＋）の付いた[**パスワード マネージャー**]アイコンが表示され、そのログオン画面用のログオンを追加するよう求められます。

1. ログオン可能なサイトでのパスワード マネージャーの動作方法をカスタマイズするには、アイコンの矢印→[**アイコンの設定**]の順にクリックします。
   - [**ログオン画面へのログオンの追加を要求**]：ログオンがまだ設定されていないログオン画面が表示されたときに、パスワード マネージャーによってログオンの追加が求められるようにするには、このオプションをクリックします。
   - [**この画面を除外する**]：パスワード マネージャーによる、このログオン画面へのログオンの追加を求めるメッセージが以後表示されないようにするには、このチェック ボックスにチェックを入れます。

     以前に除外した画面用のログオンを追加するには、以下の操作を行います。
     - 以前に除外した Web サイト ログオンまたはプログラム ページが表示されているときに、[HP ProtectTools Security Manager]ダッシュボードを開き、[**パスワード マネージャー**]をクリックします。
     - [**ログオンの追加**]をクリックします。

       [ログオンの追加]ダイアログ ボックスが開き、[**Current screen**]（現在の画面）フィールドに Web サイトのログオン画面またはプログラムが表示されます。
     - [**続行**]をクリックします。

       [[パスワード マネージャー]へのログオンの追加]画面が表示されます。
     - 画面に表示される説明に沿って操作します。詳しくは、31 ページの「ログオン情報の追加」を参照してください。
     - [**パスワード マネージャー**]アイコンは、Web サイト ログオンまたはプログラム画面が開かれるたびに表示されます。
2. ログオン画面へのログオンの追加要求を表示するオプションを無効にするには、チェック ボックスにチェックを入れます。
3. パスワード マネージャーの詳細設定にアクセスするには、[HP ProtectTools Security Manager]ダッシュボードで[**パスワード マネージャー**]→[**設定**]の順にクリックします。

VeriSign Identity Protection（VIP）

VeriSign VIP 対応の Web サイトで使用するための VeriSign VIP アクセス トークンを作成できます。これらのトークンは、パスワード マネージャーが自動ログオンを作成するために使用します。VeriSign VIP 対応のログオン画面にドラッグ アンド ドロップされたり指定フィールドに手動で入力されたりしたトークンは、この自動ログオンに統合されます。

VeriSign VIP を有効にし、[HP ProtectTools Security Manager]ダッシュボードから、または任意の VeriSign VIP 対応 Web サイトでトークンを作成できます。トークンを使用するには、当該 Web サイトで使用するトークンを登録する必要があります。

トークンを登録して最初に使用した後、（任意で）通常のログオン資格情報にトークンを付加し、資格情報と共に送信できます。トークンの付加を許可しないサイトでは、トークン情報をドラッグ アンド ドロップするか、手動で入力できます。

[HP ProtectTools Security Manager]ダッシュボードから VeriSign VIP を有効にし、VeriSign VIP トークンを作成するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードを開きます。詳しくは、27 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. [**パスワード マネージャー**]→[**VIP**]の順にクリックします。
3. [**VIP の取得**]をクリックします。

   VeriSign VIP トークンが作成され、[VeriSign VIP]ページに表示されます。トークンは、今後このページにアクセスするたびに表示されます。

Web サイトから VeriSign VIP を有効にし、VeriSign VIP トークンを作成するには、以下の操作を行います。

1. VeriSign VIP 対応の Web サイトにアクセスするたびに、パスワード マネージャーが警告メッセージを表示します。
2. 画面用のログオンを作成します。詳しくは、31 ページの「ログオン情報の追加」を参照してください。
3. [ログオンの作成]ダイアログ ボックスで、[**I want additional account protection with VIP**]（VIP によるアカウント保護を追加する）を選択します。

Web サイト用の VeriSign VIP トークンを登録するには、以下の操作を行います。

1. VeriSign VIP 対応の Web サイトに、手動またはパスワード マネージャーのログオンでログオンします。
2. 表示される VeriSign VIP バルーンをクリックして、このサイト用のログオンを作成します。
3. [[パスワード マネージャー]へのログオンの追加]ダイアログ ボックスで、[**I want VIP security on this site**]（このサイトで VIP セキュリティを使用する）を選択します。

   このオプションは、VeriSign VIP セキュリティが使用可能なサイトに対してのみ表示されます。サイトでサポートされている場合は、通常の認証方法と共に VIP セキュリティ コードが自動的に入力されるように選択することもできます。

設定

HP ProtectTools Security Manager では、以下の個人設定を指定できます。

1. [**ログオン画面へのログオンの追加を要求**]：Web サイトまたはプログラムのログオン画面が検出されるたびに[**パスワード マネージャー**]アイコンをプラス記号（＋）付きで表示し、この画面のログオンを追加してパスワードを保管できることを示します。この機能を無効にするには、[アイコンの設定]ダイアログ ボックスで[**ログオン画面へのログオンの追加を要求**]の横にあるチェック ボックスのチェックを外します。
2. [**Open Password Manager with ctrl+win+h**]（ctrl ＋ win ＋ h でパスワード マネージャーを開く）：パスワード マネージャーの[**クイック リンク**]メニューを開くための初期設定のホットキーは、ctrl ＋ Windows ロゴ キー＋ h です。このホットキーを変更するには、このオプションをクリックして新しいキーの組み合わせを入力します。ctrl、alt、shift、および任意の英数字キーを組み合わせることができます。
3. [**適用**]をクリックして変更を保存します。

Credential Manager

Security Manager の証明情報を使用して、ユーザーが本人であることを確認します。このコンピューターの管理者は、Windows アカウント、Web サイト、またはプログラムにログオンするユーザーが証明情報の確認に使用できる証明情報の種類を設定できます。

使用できる証明情報は、このコンピューターに内蔵または接続されているセキュリティ デバイスの種類によって異なります。[**マイ ログオン**]の下の[**Credential Manager**]をクリックするとサポートされている証明情報、要件、および現在の状態が一覧表示されるほか、以下のどれかまたはすべての情報が含まれます。

- パスワード
- HP SpareKey
- 指紋
- スマート カード
- 顔

証明情報を登録または変更するには、その証明情報のリンクをクリックし、画面の説明に沿って操作します。

Windows パスワードの変更

HP ProtectTools Security Manager を使用すると、Windows の[コントロール パネル]を使用するよりも、すばやく簡単に Windows パスワードを変更できます。

Windows パスワードを変更するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードで、[**Credential Manager**]→[**パスワード**]の順にクリックします。
2. [**現在の Windows パスワード**]テキスト ボックスに、現在のパスワードを入力します。
3. [**新しい Windows パスワード**]テキスト ボックスに新しいパスワードを入力し、[**新しいパスワードの確認**]テキスト ボックスにそのパスワードを再度入力します。
4. [**変更**]をクリックすると、現在のパスワードが、入力した新しいパスワードにすぐに変更されます。

HP SpareKey のセットアップ

HP SpareKey を使用すると、管理者によって定義済みの一覧からセキュリティに関する 3 つの質問に回答して、（サポートされているプラットフォーム上の）コンピューターにアクセスできます。

HP ProtectTools Security Manager から、[使用開始準備]ウィザードの初期セットアップ時に個人用の HP SpareKey をセットアップするよう求めるメッセージが表示されます。

HP SpareKey をセットアップするには、以下の操作を行います。

1. ウィザードの[SpareKey]ページで、セキュリティに関する質問を 3 つ選択し、各質問の回答を入力します。
2. [**次へ**]をクリックします。

[**Credential Manager**]の下の[SpareKey]ページで、別の質問を選択したり、回答を変更したりできます。

HP SpareKey がセットアップされた後、ブート前ログオン画面または Windows の[ようこそ]画面から HP SpareKey を使用してコンピューターにアクセスできます。

指紋の登録

コンピューターに指紋認証システムが内蔵または接続されている場合は、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）は[使用開始準備]ウィザードから初期セットアップ時に指紋を設定（指紋認証システムの用語としては「登録」）するよう求めるメッセージが表示されます。[HP ProtectTools Security Manager]ダッシュボードの[**Credential Manager**]の下の[指紋]ページでも指紋を登録できます。

1. 両手の輪郭が表示されます。すでに登録されている指は緑色で強調表示されます。輪郭で示されている指をクリックします。

   注記： 以前に登録された指紋を削除するには、その指紋に対応する指をクリックします。

2. 登録する指を選択すると、指紋が正常に登録されるまでその指を滑らせるよう求められます。登録された指は、輪郭が付いて緑色で強調表示されます。
3. 少なくとも 2 本の指を登録する必要があります。人差し指または中指をおすすめします。別の指を登録するには、手順 1 および 2 を繰り返します。
4. [**次へ**]をクリックし、画面の説明に沿って操作します。

注意： この「お使いになる前に」で説明している手順で指紋を登録している場合は、[**次へ**]をクリックするまで指紋の情報が保存されません。コンピューターをしばらくアイドル状態にしていた場合や、プログラムを閉じた場合は、それ以前に行った変更が保存されません。

スマート カードのセットアップ

認証にスマート カードを使用するには、管理者が事前にスマート カードを初期化および登録する必要があります。

スマート カードの初期化

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）では、多くの種類のスマート カードがサポートされます。PIN 番号として使用できる文字の数と種類はそれぞれ異なる場合があります。通常は、HP ProtectTools でセキュリティ アルゴリズムに使用されるセキュリティ証明書および管理 PIN をインストールするためのツールがスマート カードの製造元から提供されます。

注記： ActivIdentity ソフトウェアをインストールする必要があります。

1. カードをリーダーに挿入します。
2. [**スタート**]→[**すべてのプログラム**]→[**ActivClient PIN Initialization Tool**]（ActivClient PIN 初期化ツール）の順に選択します。
3. PIN を入力し、確認用に再入力します。
4. [**次へ**]をクリックします。

スマート カード ソフトウェアによってロック解除キーが提供されます。ほとんどのスマート カードでは、PIN を 5 回続けて間違って入力すると、カードが自動的にロックされます。このキーは、カードのロックを解除するために使用します。

5. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。

6. [**証明情報**]→[**スマート カード**]の順にクリックします。

7. [**管理**]タブをクリックします。

8. [**スマート カードのセットアップ**]が選択されていることを確認します。

9. PIN を入力し、[**適用**]をクリックしてから、画面の説明に沿って操作します。

10. スマート カードが正しく初期化されたら、スマート カードを登録する必要があります。

スマート カードの登録

スマート カードを初期化したら、HP ProtectTools 管理者コンソールでカードを認証方法として登録する必要があります。

1. [**Central Management**]（集中管理）の[**Setup Wizard**]（セットアップ ウィザード）をクリックします。

2. [**ようこそ**]ページで[**次へ**]をクリックして、Windows パスワードを入力します。

3. [**SpareKey**]ページで、[**[HP SpareKey]のセットアップのスキップ**]をクリックします（SpareKey 情報を更新しない場合）。

4. [**セキュリティ機能を有効にする**]ページで、[**次へ**]をクリックします。

5. [**資格情報の選択**]ページで、[**スマート カードのセットアップ**]が選択されていることを確認して、[**次へ**]をクリックします。

6. [**スマート カード**]ページで、PIN を入力して、[**次へ**]をクリックします。

7. [**完了**]をクリックします。

スマート カードは Security Manager で登録することもできます。詳しくは、Security Manager for HP ProtectTools ソフトウェアのヘルプを参照してください。

スマート カードの設定

コンピューターにスマート カード リーダーがインストールまたは接続されている場合、[スマート カード]ページに 2 つのタブが表示されます。

- ［**設定**］：スマート カードが取り外されたときは、自動的にロックするようにコンピューターを設定します。

  注記： コンピューターがロックするのは、そのスマート カードが Windows へのログオン時の認証証明情報として使用されていた場合のみです。Windows へのログオンに使用されていなかったスマート カードを取り外しても、コンピューターはロックされません。

- ［**管理**］：以下のオプションから選択します。
  - ［**スマート カードの初期化**］：HP Protect Tools で使用するためにスマート カードを準備します。HP ProtectTools 以外で初期化され、非対称のキーペアと関連する証明書を含んでいるスマート カードを使用する場合は、特定の証明書による初期化が必要でない限り、再度初期化する必要はありません。
  - ［**スマート カードの暗証番号の変更**］：スマート カードで使用する PIN を変更できます。
  - ［**HP ProtectTools データのみを消去**］：カードの初期化中に作成される HP ProtectTools 証明書のみを消去します。その他のデータはカードから消去されません。
  - ［**スマート カードのすべてのデータの消去**］：指定されたスマート カードのすべてのデータを消去します。カードは、HP ProtectTools またはその他のアプリケーションで使用できなくなります。

注記： スマート カードによってサポートされていない機能は使用できません。

▲ ［**適用**］をクリックします。

顔認証ログオンのシーンの登録

コンピューターに Web カメラが内蔵または接続されている場合は、HP ProtectTools Security Manager は[使用開始準備]ウィザードから初期セットアップ時にシーンを設定（顔認証の用語としては「登録」）するよう要求するメッセージが表示されます。[HP ProtectTools Security Manager]ダッシュボードの［**Credential Manager**］の下の[顔]のログオン ページでもシーンを登録できます。

顔認証ログオンを使用するには、1 つ以上のシーンを登録する必要があります。正しく登録した後でも、以下の条件の 1 つ以上が変わったためにログオンが難しくなった場合には、新しいシーンを登録できます。

- 前回登録したときから顔つきが大きく変わった。
- 以前に登録したときと周囲の明るさが大幅に異なる。
- 前回の登録時に眼鏡をかけていた（またはかけていなかった）。

注記： シーンをうまく登録できない場合は、Web カメラにもっと近づいてください。

[使用開始準備]ウィザードからシーンを登録するには、以下の操作を行います。

1. ウィザードの[顔]ページで、［**詳細設定**］をクリックし、追加のセキュリティを設定します。詳しくは、42 ページの「詳細ユーザー設定」を参照してください。
2. ［**OK**］をクリックします。

3. [**開始**]をクリックするか、以前にシーンを登録したことがある場合は、[**新しいシーンの登録**]をクリックします。
4. 追加のセキュリティ オプションを選択しなかった場合は、追加のセキュリティ オプションを選択するよう求めるメッセージが表示されます。画面の説明に沿って操作し、[**次へ**]をクリックします。詳しくは、42 ページの「詳細ユーザー設定」を参照してください。
5. [**カメラ**]アイコンをクリックし、画面の説明に沿って操作して、シーンを登録します。

   画面の説明に沿って操作し、シーンを撮影している間、自分の画像を見るようにしてください。
6. [**次へ**]をクリックします。
7. [**完了**]をクリックします。

[HP ProtectTools Security Manager]ダッシュボードからもシーンを登録できます。

1. [HP ProtectTools Security Manager]ダッシュボードを開きます。詳しくは、27 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. [**マイ ログオン**]で、[**Credential Manager**]→[**顔**]の順にクリックします。
3. [**詳細設定**]をクリックし、追加のセキュリティを設定します。詳しくは、42 ページの「詳細ユーザー設定」を参照してください。
4. [**OK**]をクリックします。
5. [**開始**]をクリックするか、以前にシーンを登録したことがある場合は、[**新しいシーンの登録**]をクリックします。
6. 追加のセキュリティ オプションを選択しなかった場合は、追加のセキュリティ オプションを選択するよう求めるメッセージが表示されます。画面の説明に沿って操作し、[**次へ**]をクリックします。詳しくは、42 ページの「詳細ユーザー設定」を参照してください。
7. [**カメラ**]アイコンをクリックし、画面の説明に沿って操作して、シーンを登録します。

   画面の説明に沿って操作し、シーンを撮影している間、自分の画像を見るようにしてください。

詳細については、[顔]のログオン ページの右上にある青色の[**?**]アイコンをクリックして、Face Recognition ソフトウェアのヘルプを参照してください。

詳細ユーザー設定

追加のセキュリティが選択されていない場合、これらのオプションは[セキュリティの強化]ページにも表示されます。

1. [HP ProtectTools Security Manager]ダッシュボードを開きます。詳しくは、27 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ［**マイ ログオン**］で、［**Credential Manager**］→［**顔**］の順にクリックします。
3. ［**詳細設定**］をクリックし、以下のセキュリティ オプションを設定します。
   a. ［**セキュリティ**］タブ：以下のオプションのどれかを選択します。
      - ［**セキュリティを強化しない**］：顔認証ログオンのセキュリティを強化しない場合は、このオプションを選択します。
      - ［**PIN を使用してセキュリティを強化する**］：顔認証ログオンでユーザー専用の PIN の入力を求められるようにするには、このオプションを選択します。
         ◦ ［**PIN の作成**］をクリックします。
         ◦ Windows パスワードを入力します。
         ◦ 新しい PIN を入力してから、もう一度その PIN を入力して確認します。

         PIN が作成されたら、［**PIN の変更**］、［**PIN のリセット**］、または［**PIN の削除**］オプションを選択できます。
      - ［**Bluetooth を使用してセキュリティを強化する**］：Bluetooth®対応電話と Face Recognition をペアリングするには、このオプションを選択します。Windows ログオンの実行中に顔が認証されると、Face Recognition はペアリングされた Bluetooth 電話の存在も確認します。電話が存在し、Bluetooth が有効になっていれば、Windows へのログオンが許可されます。
         ◦ Bluetooth がコンピューターと電話の両方で有効になっていることを確認します。

         Bluetooth 対応電話が存在しない場合、ペアリングされた Bluetooth 対応電話を有効にし、ログオン プロセスを再開するよう求めるメッセージが表示されます。30 秒後、Face Recognition のログオン ウィンドウが一時停止します。ログオン プロセスを開始するには、［**カメラ**］アイコンをクリックします。Bluetooth 対応電話が存在しない場合、通常の Windows パスワードを使用してログオンできます。
         ◦ ［**追加**］をクリックします。
         ◦ Bluetooth デバイスが表示されたら、選択して、［**次へ**］をクリックします。

［**OK**］をクリックします。

b. ［**その他の設定**］タブ：以下の 1 つ以上のオプションを有効にするには、チェック ボックスにチェックを入れます。また、オプションを無効にするには、チェック ボックスのチェックを外します。これらの設定は現在のユーザーにのみ適用されます。

- ［**顔認識のイベントでサウンドを再生する**］：顔認証ログオンが成功または失敗したときに音を鳴らします。
- ［**ログオンに失敗したら、シーンの更新を要求する**］：顔認証ログオンには失敗してもパスワードの入力には成功した場合に、今後の顔認証ログオンが成功する確率を高めるためにさまざまな画像を保存するよう求めるメッセージが表示されます。
- ［**ログオンに失敗したら、新しいシーンの登録を要求する**］：顔認証ログオンには失敗してもパスワードの入力には成功した場合は、今後の顔認証ログオンが成功する確率を高めるために新しいシーンを保存するよう求められることがあります。

［**OK**］をクリックします。

個人用 ID カード

ID カードは、ユーザーの名前およびユーザーが選択した写真を表示して、Windows アカウントの所有者を一意に識別します。ID カードは、Security Manager の各ページの左上隅に、目立つような形で表示されます。

画像および名前の表示方法は変更できます。初期設定では、Windows のセットアップ中に選択した完全な Windows ユーザー名および画像が表示されます。

表示名を変更するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードを開きます。詳しくは、27 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ダッシュボードの左上隅にある ID カードをクリックします。
3. このアカウントの Windows ユーザー名を表示するボックスをクリックし、新しい名前を入力して、**[保存]**ボタンをクリックします。

表示画像を変更するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードを開きます。詳しくは、27 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ダッシュボードの左上隅にある ID カードをクリックします。
3. **[画像の選択]**→画像→**[保存]**の順にクリックします。

オプションの設定

HP ProtectTools Security Manager では、個人設定を指定できます。[HP ProtectTools Security Manager]ダッシュボードで、**[詳細設定]**→**[設定]**の順にクリックします。使用可能な設定が、[全般]と[指紋]の 2 つのタブに表示されます。

[全般]タブ

[外観]：**[タスク バーの通知領域にアイコンを表示する]**

- タスク バーへのアイコンの表示を有効にするには、このチェック ボックスにチェックを入れます。
- タスク バーへのアイコンの表示を無効にするには、このチェック ボックスのチェックを外します。

[指紋]タブ

注記： [**指紋**]タブは、コンピューターに指紋認証システムおよび正しいドライバーがインストールされている場合にのみ表示されます。

- [**クイック アクション**]：クイック アクションを使用すると、割り当てたキーを押したまま、指を滑らせて指紋を読み取らせたときに実行される HP ProtectTools Security Manager のタスクを選択できます。

  クイック アクションを一覧のどれかのキーに割り当てるには、[（**キー**）＋**指紋**]オプションをクリックして、使用可能なタスクをメニューから 1 つ選択します。

- [**指紋スキャンのフィードバック**]：指紋認証システムが使用できる場合にのみ表示されます。この設定を使用すると、指紋を読み取らせたときに返されるフィードバックを調整できます。
  - [**サウンド フィードバックを有効にする**]：指紋が読み取られたときに、Security Manager によってサウンドのフィードバックが返されます。プログラム イベントごとに異なるサウンドが再生されます。Windows の[コントロール パネル]の[**サウンド**]タブでイベントに新しいサウンドを割り当てるか、このオプションを選択解除してサウンドのフィードバックを無効にできます。
  - [**スキャン品質フィードバックを表示する**]

    品質に関係なくすべての読み取りを表示するには、このチェック ボックスにチェックを入れます。

    高品質の読み取りのみを表示するには、このチェック ボックスのチェックを外します。

データのバックアップおよび復元

Security Manager のデータは定期的にバックアップすることをおすすめします。バックアップの頻度は、データが変更される頻度によって決まります。たとえば、毎日のように新しいログオンを追加している場合は、データを毎日バックアップする必要があります。

また、他のコンピューターへの移行時にバックアップを使用することもできます。この作業は、インポートおよびエクスポートと呼ばれます。

注記： この機能によってバックアップされるのはデータのみです。

バックアップ ファイルからデータを復元できるようにするには、バックアップ データを取り込むコンピューターに HP ProtectTools Security Manager をインストールしておく必要があります。

データをバックアップするには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードを開きます。詳しくは、27 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。
2. ダッシュボードの左側のパネルで、[**詳細設定**]→[**バックアップおよび復元**]の順にクリックします。
3. [**データのバックアップ**]をクリックします。
4. バックアップに含めるモジュールを選択します。多くの場合、すべてのモジュールを選択します。
5. ID を検証します。
6. ストレージ ファイルの名前を入力します。初期設定では、このファイルはユーザーの[ドキュメント]フォルダーに保存されます。別の場所を指定するには、[**参照**]をクリックします。

7. ファイルを保護するためのパスワードを入力します。

8. [**完了**]をクリックします。

データを復元するには、以下の操作を行います。

1. [HP ProtectTools Security Manager]ダッシュボードを開きます。詳しくは、27 ページの「Security Manager（セキュリティ マネージャー）を開く」を参照してください。

2. ダッシュボードの左側のパネルで、[**詳細設定**]→[**バックアップおよび復元**]の順にクリックします。

3. [**データの復元**]をクリックします。

4. 以前に作成したストレージ ファイルを選択します。表示されているフィールドにパスを入力して、[**参照**]をクリックします。

5. ファイルを保護するために使用しているパスワードを入力します。

6. データを復元するモジュールを選択します。多くの場合、表示されるすべてのモジュールを選択します。

7. Windows パスワードを検証します。

8. [**完了**]をクリックします。

5 Drive Encryption for HP ProtectTools（一部のモデルのみ）

Drive Encryption for HP ProtectTools は、コンピューターのハードドライブを暗号化することによって完全なデータ保護を可能にします。Drive Encryption を有効にしている場合は、Windows オペレーティング システムが起動する前に表示される、Drive Encryption のログイン画面からログインする必要があります。

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のセットアップ ウィザードを使用すると、Windows 管理者は、Drive Encryption の有効化、暗号化キーのバックアップ、およびドライブの選択または選択解除を行えます。詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

Drive Encryption では、以下のタスクを実行できます。

- Drive Encryption の設定の選択：
  - TPM で保護されたパスワードの有効化
  - ソフトウェアによる暗号化を使用した個々のドライブまたはパーティションの暗号化または暗号化の解除
  - ハードウェアによる暗号化を使用した自己暗号化ドライブの暗号化または暗号化の解除
  - Drive Encryption のブート前認証が常に要求されるようにスリープまたはスタンバイ状態を無効にすることによる、一層のセキュリティ強化

注記： 暗号化できるドライブは内蔵 SATA ハードドライブおよび外付け eSATA ハードドライブのみです。

- バックアップ キーの作成
- Drive Encryption キーの復元
- パスワード、登録された指紋、またはスマートカードの PIN を使用した Drive Encryption のブート前認証の有効化

Drive Encryption を開く

管理者は HP ProtectTools 管理者コンソールから Drive Encryption にアクセスできます。

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側の枠内で、[**Drive Encryption**]をクリックします。

一般的なタスク

標準ハードドライブに対する Drive Encryption の有効化

標準ハードドライブはソフトウェアによる暗号化を使用して暗号化されます。Drive Encryption を有効にするには、以下の操作を行います。

1. Drive Encryption を有効にするには、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のセットアップ ウィザードを使用します。
2. 画面の説明に沿って操作し、[**セキュリティ機能を有効にする**]ページが表示されたら、手順 4 に進みます。

または

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**セキュリティ**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**機能**]をクリックします。
4. [**Drive Encryption**]チェック ボックスにチェックを入れ、[**次へ**]をクリックします。

   注記： 暗号化するハードドライブが選択されていない場合、Drive Encryption のブート前認証は有効になりますが、ドライブは暗号化されません。

5. [**暗号化するドライブ**]で、暗号化するハードドライブのチェック ボックスにチェックを入れ、[**次へ**]をクリックします。
6. 暗号化キーをバックアップするには、適切なスロットにストレージ デバイスを挿入します。

   注記： 暗号化キーを保存するには、FAT32 でフォーマットされた USB ストレージ デバイスを使用する必要があります。バックアップにはフロッピー ディスク、USB メモリ スティック、SD（Secure Digital）メモリ カード、または MMC を使用できます。

7. [**Drive Encryption キーのバックアップ**]で、暗号化キーを保存するストレージ デバイスのチェック ボックスにチェックを入れます。
8. [**次へ**]をクリックします。

   注記： コンピューターが再起動されます。

Drive Encryption が有効になりました。ドライブのサイズによっては、ドライブの暗号化に何時間もかかることがあります。

詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

自己暗号化ドライブに対する Drive Encryption の有効化

自己暗号化ドライブの管理に関する Trusted Computing Group の OPAL 仕様に適合する自己暗号化ドライブは、ソフトウェアによる暗号化またはハードウェアによる暗号化を使用して暗号化できます。自己暗号化ドライブに対して Drive Encryption を有効にするには、以下の操作を行います。

1. Drive Encryption を有効にするには、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のセットアップ ウィザードを使用します。
2. 画面の説明に沿って操作し、[**セキュリティ機能を有効にする**]ページが表示されたら、次の「ソフトウェアによる暗号化」または「ハードウェアによる暗号化」の手順 4 に進みます。

注記： 自己暗号化ドライブの管理に関する Trusted Computing Group の OPAL 仕様に適合する自己暗号化ドライブがお使いのコンピューターに搭載されていない場合は、ハードウェアによる暗号化のオプションは使用できず、初期設定でソフトウェアによる暗号化が使用されます。

自己暗号化ドライブと標準ハードドライブが混在している場合も、ハードウェアによる暗号化のオプションは使用できず、初期設定でソフトウェアによる暗号化が使用されます。

または

ソフトウェアによる暗号化

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**セキュリティ**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**機能**]をクリックします。
4. [**Drive Encryption**]チェック ボックスにチェックを入れ、[**次へ**]をクリックします。
5. [**暗号化するドライブ**]で、暗号化するハードドライブのチェック ボックスにチェックを入れ、[**次へ**]をクリックします。
6. 暗号化キーをバックアップするには、適切なスロットにストレージ デバイスを挿入します。

   注記： 暗号化キーを保存するには、FAT32 でフォーマットされた USB ストレージ デバイスを使用する必要があります。バックアップにはフロッピー ディスク、USB メモリ スティック、SD（Secure Digital）メモリ カード、または MMC を使用できます。

7. [**Drive Encryption キーのバックアップ**]で、暗号化キーを保存するストレージ デバイスのチェック ボックスにチェックを入れます。
8. [**適用**]をクリックします。

   注記： コンピューターが再起動されます。

   Drive Encryption が有効になりました。ドライブのサイズによっては、ドライブの暗号化に何時間もかかることがあります。

ハードウェアによる暗号化

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**セキュリティ**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**機能**]をクリックします。
4. [**Drive Encryption**]チェック ボックスにチェックを入れ、[**次へ**]をクリックします。

   注記： ドライブが 1 つだけ表示される場合は、そのドライブのチェック ボックスが自動的に選択され、グレーで表示されます。

   複数のドライブが表示される場合は、それらのドライブのチェック ボックスが自動的に選択されますが、グレーにはなりません。

   [**次へ**]ボタンは 1 つ以上のドライブが選択されるまで使用できません。

5. 画面下部の[**ドライブのハードウェア暗号化を使用**]チェック ボックスにチェックが入っていることを確認してください。
6. [**暗号化するドライブ**]で、暗号化するハードドライブのチェック ボックスにチェックを入れ、[**次へ**]をクリックします。
7. 暗号化キーをバックアップするには、適切なスロットにストレージ デバイスを挿入します。

   注記： 暗号化キーを保存するには、FAT32 でフォーマットされた USB ストレージ デバイスを使用する必要があります。バックアップにはフロッピー ディスク、USB メモリ スティック、SD（Secure Digital）メモリ カード、または MMC を使用できます。

8. [**Drive Encryption キーのバックアップ**]で、暗号化キーを保存するストレージ デバイスのチェック ボックスにチェックを入れます。
9. [**適用**]をクリックします。

   注記： コンピューターを再起動する必要があります。

   Drive Encryption が有効になりました。ドライブの暗号化に数分かかることがあります。

詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

Drive Encryption の無効化

管理者は、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のセットアップ ウィザードを使用して Drive Encryption を無効にできます。詳しくは、HP ProtectTools Security Manager ソフトウェアのヘルプを参照してください。

▲ 画面の説明に沿って操作し、[**セキュリティ機能を有効にする**]ページが表示されたら、手順 4 に進みます。

または

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
2. 左側のパネルで、[**セキュリティ**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**機能**]をクリックします。
4. [**Drive Encryption**]チェック ボックスのチェックを外し、[**次へ**]をクリックします。

   Drive Encryption の無効化が開始されます。

   注記： ソフトウェアによる暗号化が使用されていた場合は、暗号化の解除が開始されます。ドライブのサイズによっては、暗号化の解除に何時間もかかることがあります。暗号化の解除が完了すると、Drive Encrytion が無効になります。

   ハードウェアによる暗号化が使用されていた場合は、ドライブの暗号化がすぐに解除され（数分かかることがあります）、その後 Drive Encryption が無効になります。

   ドライブが無効化された後、コンピューターを再起動する必要があります。

Drive Encryption の有効化後のログイン

Drive Encryption が有効になり、ユーザ アカウントが登録された後でコンピュータを起動した場合、Drive Encryption のログイン画面からログインする必要があります。

注記： ハードウェアによる暗号化のシナリオでは、必ずコンピューターの電源を切ってください。コンピューターの電源を切らないでコンピューターを再起動した場合、Drive Encryption のブート前認証画面は表示されません。

注記： スリープまたはスタンバイ状態を無効にしないと、それらの状態から復帰するときに、ソフトウェアによる暗号化でもハードウェアによる暗号化でも Drive Encryption のブート前認証が表示されません。

ハイバネーション状態から復帰するときは、Drive Encryption のブート前認証が表示されます。

注記： Windows 管理者が HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）で[ブート前セキュリティ]を有効にしている場合は、Drive Encryption のログイン画面ではなく、コンピューターが起動した直後にコンピューターにログインできます。

1. ユーザー名をクリックし、Windows のパスワードまたはスマート カードの PIN を入力するか、または登録した指の指紋を認証システムで読み取らせます。

   注記： 以下のスマート カードがサポートされます。

スマート カード

- ActivIdentity 64K V2C スマート カード
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB key V3.0 ZFG-48001-A

PCMCIA リーダー

- Express Card 54 SCR3340 内蔵リーダー
- SCR 201
- SCR 243（HP ブランドでもあります）
- ActivCard
- Omnikey 4040
- Cisco

USB リーダー

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- HP スマート カード端末

2. [**OK**]をクリックします。

注記： Drive Encryption のログイン画面で復元キーを使用してログインする場合は、Windows のログイン画面で、パスワード、スマート カードの PIN、または登録した指紋を使用して認証することを要求されます。

ハードドライブの暗号化によるデータの保護

HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のセットアップウィザードでハードドライブを暗号化してデータを保護することを強くおすすめします。

1. 左側のパネルで、[**Drive Encryption**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
2. [**設定**]をクリックします。
3. ソフトウェアによって暗号化するドライブについては、暗号化するドライブ パーティションを選択します。

   注記： これは、1 つ以上の標準ハードドライブと 1 つ以上の自己暗号化ドライブが存在する混合ドライブのシナリオにも該当します。

または

▲ ハードウェアによって暗号化するドライブについては、暗号化するドライブを選択します。少なくとも 1 つのドライブを選択する必要があります。

暗号化の状態の表示

ユーザーは HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）で暗号化の状態を表示できます。

注記： 管理者は HP ProtectTools 管理者コンソールを使用して Drive Encryption の状態を変更できます。

1. HP ProtectTools Security Manager を起動します。
2. ［**マイ データ**］で［**Drive Encryption**］をクリックします。

   ソフトウェアによる暗号化のシナリオでは、［**ドライブの状態**］に以下のどれかの状態コードが表示されます。

   - 有効
   - 無効
   - 暗号化されていない
   - 暗号化されている
   - 暗号化を実行中
   - 暗号化解除を実行中

   ハードウェアによる暗号化のシナリオでは、［**ドライブの状態**］に次の状態コードが表示されます。

   - 暗号化されている

   ハードドライブの暗号化または暗号化解除を実行中、暗号化または暗号化解除が完了した割合および完了するまでの残り時間が進行状況バーに表示されます。

高度なタスク

Drive Encryption の管理（管理者のタスク）

管理者は[Drive Encryption]の下の[設定]ページで、Drive Encryption の状態（有効、無効、またはハードウェアによる暗号化が有効）を表示および変更し、コンピューター上のすべてのハードドライブの暗号化の状態を表示できます。

注記： ハードウェアによる暗号化は[設定]ページでは変更できません。

- 状態が無効の場合、Drive Encryption は Windows 管理者によって有効にされておらず、ハードドライブは保護されていません。Drive Encryption を有効にするには、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）のセットアップ ウィザードを使用します。
- 状態が有効の場合、Drive Encryption は有効にされ、設定されています。ドライブは、次のどれかの状態になっています。

ソフトウェアによる暗号化

- 暗号化されていない
- 暗号化されている
- 暗号化を実行中
- 暗号化解除を実行中

ハードウェアによる暗号化

- 暗号化されている

個々のドライブの暗号化または暗号化の解除（ソフトウェアによる暗号化のみ）

管理者は[設定]ページを使用して、コンピューター上の 1 つまたは複数のハードドライブを暗号化するか、またはすでに暗号化されているドライブの暗号化を解除することができます。

1. HP ProtectTools 管理者コンソールを開きます。
2. 左側のパネルで、[**Drive Encryption**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**設定**]をクリックします。
4. [**ドライブの状態**]で、暗号化するか、または暗号化を解除する各ハードドライブの横にあるチェック ボックスにチェックを入れるか、またはチェックを外して、[**適用**]をクリックします。

注記： ドライブの暗号化または暗号化解除が行われている間、現在のセッションで処理が完了するまでの残り時間が進行状況バーに表示されます。

暗号化中にコンピューターをシャットダウンするか、スリープ、スタンバイ、またはハイバネーションを開始し、その後起動しなおした場合、進行状況バーの残り時間はリセットされますが、実際の暗号化は直前に停止した場所から再開されます。パーセントで表示される進行状況バーと残り時間の表示がすばやく進み、現在の進行状況が反映されます。

注記： ダイナミック パーティションはサポートされていません。パーティションが使用可能として表示されるが、選択しても暗号化できない場合、そのパーティションはダイナミック パーティションです。ダイナミック パーティションは、[ディスクの管理]で新しいパーティションを作成するためにどれかのパーティションを縮小した結果生成されます。

パーティションがダイナミック パーティションに変換される場合は、警告が表示されます。

バックアップおよび復元（管理者のタスク）

Drive Encryption が有効な場合、管理者は[暗号化キーのバックアップ]ページを使用して暗号化キーをリムーバブル メディアにバックアップしたり、復元を実行したりできます。

暗号化キーのバックアップ

管理者は、暗号化されたドライブの暗号化キーをリムーバブル ストレージ デバイスにバックアップできます。

⚠ 注意： バックアップ キーを含むストレージ デバイスは必ず安全な場所に保管してください。パスワードを忘れたり、スマート カードを紛失したり、指紋を登録していない場合に、このデバイスがハードドライブにアクセスする唯一の方法となります。

1. HP ProtectTools 管理者コンソールを開きます。
2. 左側のパネルで、[**Drive Encryption**]の左にある[**+**]アイコンをクリックして、使用可能なオプションを表示します。
3. [**暗号化キーのバックアップ**]をクリックします。
4. 暗号化キーのバックアップに使用するストレージ デバイスを挿入します。
5. [**ドライブ**]で、暗号化キーをバックアップするデバイスのチェック ボックスにチェックを入れます。
6. [**キーをバックアップする**]をクリックします。
7. 表示されるページに記載されている情報を読み、[**次へ**]をクリックします。選択したストレージ デバイスに暗号化キーが保存されます。

暗号化キーの復元

管理者は、以前に暗号化キーを保存したリムーバブル ストレージ デバイスから暗号化キーを復元できます。

1. コンピュータの電源を入れます。
2. バックアップ キーが保管されているリムーバブル ストレージ デバイスを装着します。
3. Drive Encryption for HP ProtectTools のログイン ダイアログ ボックスが表示されたら、[**オプション**]をクリックします。
4. [**復元**]をクリックします。
5. バックアップ キーが含まれているファイルを選択するか、[**参照**]をクリックして該当のファイルを探してから、[**次へ**]をクリックします。
6. 確認ダイアログ ボックスが表示されたら、[**OK**]をクリックします。

コンピュータが起動します。

注記： 復元を実行した後は、パスワードを再設定することを強くおすすめします。

6 Privacy Manager for HP ProtectTools（一部のモデルのみ）

Privacy Manager for HP ProtectTools を使用すると、電子メールまたは Microsoft Office ドキュメントを使用するときに、高度なセキュリティ ログイン（認証）方法を使用して、通信の発信元、整合性、セキュリティを確認できます。

Privacy Manager では、HP ProtectTools Security Manager が提供するセキュリティ インフラストラクチャを活用します。HP ProtectTools Security Manager のセキュリティ ログイン方法は、以下のとおりです。

- 指紋認証
- Windows のパスワード
- スマート カード
- 顔認識

Privacy Manager では、上記のセキュリティ ログイン方法を使用できます。

Privacy Manager の起動

Privacy Manager を起動するには、以下の操作を行います。

- Microsoft Outlook で Microsoft Outlook 固有の機能を使用するには、[**メッセージ**]タブの[**プライバシ**]グループにある[**安全に送信**]をクリックします。
- Microsoft Office ドキュメントで多くの機能を使用するには、[**ホーム**]タブの[**プライバシ**]グループにある[**署名と暗号化**]をクリックします。
- 追加の機能を使用するには、[HP ProtectTools Security Manager]ダッシュボードにアクセスします。
    - [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]→[**Privacy Manager**]の順にクリックします。

      または
    - [**HP ProtectTools**]デスクトップ ガジェット アイコンをクリックします。

      または
    - タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックしてから[**Privacy Manager**]→[**構成**]の順にクリックします。

セットアップ手順

Privacy Manager の証明書の管理

Privacy Manager の証明書は、公開キー基盤（PKI）と呼ばれる暗号化技術を使用して、データやメッセージを保護します。PKI の利用にあたり、ユーザーは暗号キーと、証明機関（CA）が発行する Privacy Manager の証明書を取得する必要があります。認証を定期的に要求するのみの多くのデータ暗号化ソフトウェアや認証ソフトウェアとは異なり、Privacy Manager は、暗号キーを使用して電子メール メッセージや Microsoft Office ドキュメントに署名するたびに認証を要求します。Privacy Manager によって、重要な情報の保存および送信の処理が安全で確実なものとなります。

Certificate Manager（証明書マネージャー）を使用すると、以下のタスクを実行できます。

- 60 ページの「Privacy Manager の証明書の要求」
- 61 ページの「事前に割り当てられた Privacy Manager の企業向け証明書の取得」
- 62 ページの「Privacy Manager の証明書の初期設定の指定」
- 61 ページの「第三者証明書のインポート」
- 62 ページの「Privacy Manager の証明書の詳細の表示」
- 62 ページの「Privacy Manager の証明書の更新」
- 62 ページの「Privacy Manager の証明書の初期設定の指定」
- 63 ページの「Privacy Manager の証明書の削除」
- 63 ページの「Privacy Manager の証明書の復元」
- 63 ページの「Privacy Manager の証明書の廃止」

Privacy Manager の証明書の要求

Privacy Manager の機能を使用するには、有効な電子メール アドレスを使用して Privacy Manager から Privacy Manager の証明書を要求し、インストールしておく必要があります。この電子メール アドレスは、Privacy Manager Certificate を要求するコンピューターの[Microsoft Outlook]のアカウントとして設定する必要があります。

1. Privacy Manager を開き、[**証明書**]をクリックします。
2. [**Privacy Manager の証明書の要求**]をクリックします。
3. [ようこそ]ページで、画面に表示される内容を確認してから[**次へ**]をクリックします。
4. [使用許諾契約]ページで、使用許諾契約の内容を確認します。
5. [**使用許諾契約の条件に同意する場合はチェック**]の隣のチェック ボックスにチェックが入っていることを確認してから、[**次へ**]をクリックします。
6. [証明書の詳細]ページで、求められた情報を入力してから[**次へ**]をクリックします。
7. [証明書の要求が承認されました]ページで、[**完了**]をクリックします。

Microsoft Outlook に、Privacy Manager の証明書が添付された電子メールが届きます。

事前に割り当てられた Privacy Manager の企業向け証明書の取得

1. Microsoft Outlook に届いている、企業向け証明書（Corporate Certificate）が割り当てられたことを示す電子メールが届いています。その電子メールを開きます。
2. [**入手**]をクリックします。

Microsoft Outlook に、Privacy Manager の証明書が添付された電子メールが届きます。

証明書をインストールするには、61 ページの「Privacy Manager の証明書の設定」を参照してください。

Privacy Manager の証明書の設定

1. Privacy Manager の証明書の添付された電子メールを受信したら、メールを開き、[**設定**]ボタンをクリックします。[設定]ボタンは、Microsoft Outlook 2007 または Microsoft Outlook 2010 の場合はメッセージの右下隅、Microsoft Outlook 2003 の場合は左上隅にあります。
2. 選択したセキュリティ ログイン方法で認証します。
3. [証明書がインストールされました]ページで、[**次へ**]をクリックします。
4. [証明書のバックアップ]ページで、バックアップ ファイルの保存先と名前を入力するか、または[**参照**]をクリックして保存先を探します。

   ⚠ **注意：** ファイルはハードドライブ以外の場所に保存し、安全な場所に保管してください。本人以外はこのファイルを使用できません。また、Privacy Manager の証明書と、関連するキーを復元しなければならない場合には、このファイルが必要です。

5. パスワードの入力と確認を行い、[**次へ**]をクリックします。
6. 選択したセキュリティ ログイン方法で認証します。
7. 信頼済み連絡先の招待の処理を始める場合は、65 ページの「Microsoft Outlook のアドレス帳を使用した信頼済み連絡先の追加」のトピックで、手順 2 から始まる画面の説明に沿って操作します。

   または

   [**キャンセル**]をクリックすると、後で信頼済み連絡先を追加できます。詳しくは、64 ページの「信頼済み連絡先の管理」を参照してください。

第三者証明書のインポート

証明書インポート ウィザードから第三者証明書を Privacy Manager にインポートできる場合があります。

この機能を使用するには、HP ProtectTools 管理者コンソールの[**Allow use of third-party certificates**]（第三者証明書の使用の許可）設定が[**Privacy Manager**]の[設定]ページで有効になっている必要があります。

1. Privacy Manager を開き、[**証明書**]をクリックします。
2. [**Certificate Manager**]（証明書マネージャー）タブを選択し、[**証明書のインポート**]をクリックします。

   証明書のインポートが許可されていない場合、このボタンは表示されません。

3. このコンピューターにすでにインストールされている証明書をインポートするか、PFX（Personal Information Exchange/PKCS#12）ファイルとして保存されている証明書をインポートするかを選択し、[**次へ**]をクリックします。

   - このコンピューターにインストールされている証明書をインポートするには、目的の証明書を選択し、[**次へ**]をクリックします。
   - PFX 証明書を選択するには、[**参照**]をクリックし、PFX ファイルの場所に移動し、[**次へ**]をクリックします。PFX ファイルのパスワードを入力して、[**次へ**]をクリックします。

4. インポート処理が完了したら、[**次へ**]をクリックします。

5. インポートした証明書をバックアップできます。

   コンピューターのハード ドライブ以外の場所に証明書をバックアップすることをおすすめします。

Privacy Manager の証明書の詳細の表示

1. Privacy Manager を開き、[**証明書**]をクリックします。
2. Privacy Manager の証明書をクリックします。
3. [**証明書の詳細**]をクリックします。
4. 詳細の確認を終えたら、[**OK**]をクリックします。

Privacy Manager の証明書の更新

Privacy Manager の証明書が有効期限に近づくと、更新が必要であることが通知されます。

1. Privacy Manager を開き、[**証明書**]をクリックします。
2. [**証明書の更新**]をクリックします。
3. 画面の説明に沿って操作し、新しい Privacy Manager の証明書を取得します。

注記： Privacy Manager の証明書の更新処理を行っても、古い Privacy Manager の証明書は置き換えられません。新しい Privacy Manager の証明書を取得したら、60 ページの「Privacy Manager の証明書の要求」に記載されている手順でインストールする必要があります。

Microsoft の認証機関（Certificate Authority）を使用して発行された企業向け証明書を使用している場合は、CA 管理者が、元の証明書と同じ秘密キーを使用して、証明書を更新するか新しい証明書を発行する必要があります。

Privacy Manager の証明書の初期設定の指定

お使いのコンピューターに別の証明機関からの証明書がインストールされている場合でも、Privacy Manager には Privacy Manager の証明書のみが表示されます。

コンピューターに Privacy Manager からインストールした Privacy Manager の証明書が複数ある場合は、どれか 1 つを初期設定の証明書として指定できます。

1. Privacy Manager を開き、[**証明書**]をクリックします。
2. 初期設定として使用する Privacy Manager の証明書をクリックしてから、[**初期値の指定**]をクリックします。
3. [**OK**]をクリックします。

注記： 初期設定の Privacy Manager の証明書を常に使用する必要はありません。Privacy Manager のさまざまな機能によって、使用する Privacy Manager の証明書を選択できます。

Privacy Manager の証明書の削除

Privacy Manager の証明書を削除すると、この証明書で暗号化したファイルを開いたり、データを表示したりすることができなくなります。間違えて Privacy Manager の証明書を削除した場合は、証明書のインストール時に作成したバックアップ ファイルを使用して証明書を復元できます。詳しくは、63 ページの「Privacy Manager の証明書の復元」を参照してください。

Privacy Manager の証明書を削除するには、以下の操作を行います。

1. Privacy Manager を開き、[**証明書**]をクリックします。
2. 削除する Privacy Manager の証明書をクリックしてから、[**詳細**]をクリックします。
3. [**削除**]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。
5. [**閉じる**]をクリックし、[**適用**]をクリックします。

Privacy Manager の証明書の復元

Privacy Manager の証明書のインストール中に、証明書のバックアップ コピーを作成するよう要求されます。バックアップ コピーの作成は、[移行]ページからも実行できます。このバックアップ コピーは、別のコンピューターへの移行時や、証明書を同一のコンピューターに復元する場合に使用できます。

1. Privacy Manager を開き、[**移行**]をクリックします。
2. [**復元**]をクリックします。
3. [移行ファイル]ページで、[**参照**]をクリックし、バックアップ処理中に作成した.dppsm ファイルを探してから、[**次へ**]をクリックします。
4. バックアップ作成時に使用したパスワードを入力して、[**次へ**]をクリックします。
5. [**完了**]をクリックします。

詳しくは、61 ページの「Privacy Manager の証明書の設定」、または74 ページの「Privacy Manager の証明書および信頼済み連絡先のバックアップ」を参照してください。

Privacy Manager の証明書の廃止

お使いの Privacy Manager の証明書のセキュリティに問題があると感じる場合、その証明書を廃止できます。

注記： Privacy Manager の証明書を廃止しても、削除はされません。この証明書は、暗号化したファイルを表示するために引き続き使用できます。

1. Privacy Manager を開き、[**証明書**]をクリックします。
2. [**詳細**]をクリックします。
3. 廃止する Privacy Manager の証明書をクリックしてから、[**廃止**]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。
5. 選択したセキュリティ ログイン方法で認証します。
6. 画面に表示される説明に沿って操作します。

信頼済み連絡先の管理

信頼済み連絡先とは、安全に通信が出来るように、互いに Privacy Manager の証明書を交換したユーザーのことです。

信頼済み連絡先マネージャーを使用すると、以下のタスクを実行できます。

- 信頼済み連絡先の詳細の表示
- 信頼済み連絡先の削除
- 信頼済み連絡先の廃止状態の確認（高度なタスク）

信頼済み連絡先の追加

信頼済み連絡先を追加するには、以下の 3 つの処理を行います。

1. 信頼済み連絡先の受信者に、電子メールで招待状を送信します。
2. 信頼済み連絡先の受信者が、この電子メールに返信します。
3. 信頼済み連絡先の受信者から返信メールを受け取ったら、[**承認**]をクリックします。

信頼済み連絡先の電子メール招待状は、個々の受信者宛てに送信することも、Microsoft Outlook のアドレス帳に記載されているすべての連絡先に送信することもできます。

以下を参照して、信頼済み連絡先を追加します。

注記： 信頼済み連絡先になるための招待状に返信するには、信頼済み連絡先の受信者のコンピューターに、Privacy Manager または代替となるクライアントがインストールされている必要があります。代替となるクライアントのインストールについて詳しくは、DigitalPersona の Web サイト http://digitalpersona.com/privacymanager/download/（英語サイト）にアクセスしてください。

信頼済み連絡先の追加

1. Privacy Manager を開き、[**信頼済み連絡先マネージャー**]→[**連絡先の招待**]の順にクリックします。

   または

   Microsoft Outlook で、ツールバーの[**安全に送信**]の横にある下向きの矢印をクリックしてから、[**連絡先の招待**]をクリックします。

2. [証明書の選択]ダイアログ ボックスが表示された場合は、使用する Privacy Manager の証明書をクリックしてから[**OK**]をクリックします。

3. [信頼済み連絡先の招待]ダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから[**OK**]をクリックします。

   自動的に電子メールが生成されます。

4. 信頼済み連絡先に追加する受信者の電子メール アドレスを入力します。

5. テキストを編集し、自分の名前を署名します（オプション）。

6. [**送信**]をクリックします。

   注記： Privacy Manager の証明書を取得していない場合、信頼済み連絡先要求の送信には Privacy Manager の証明書が必要というメッセージが表示されます。[**OK**]をクリックして、[証明書の要求ウィザード]を起動します。詳しくは、60 ページの「Privacy Manager の証明書の要求」を参照してください。

7. 選択したセキュリティ ログイン方法で認証します。

   注記： 信頼済み連絡先の受信者は、電子メールを受信すると、電子メールを開いて右下隅の[**承認**]をクリックし、確認用のダイアログ ボックスが表示されたら[**OK**]をクリックする必要があります。

8. 信頼済み連絡先になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の[**承認**]をクリックします。

   ダイアログ ボックスが開き、受信者が信頼済み連絡先の一覧に正常に追加されたことを確認できます。

9. [**OK**]をクリックします。

Microsoft Outlook のアドレス帳を使用した信頼済み連絡先の追加

1. Privacy Manager を開き、[**信頼済み連絡先マネージャー**]→[**連絡先の招待**]の順にクリックします。

   または

   Microsoft Outlook で、ツールバーの[**安全に送信**]の横にある下向きの矢印をクリックしてから、[**Invite My Outlook Contacts**]（Microsoft Outlook の連絡先を招待）をクリックします。

2. [信頼済み連絡先の招待]ページが開いたら、信頼済み連絡先に追加する受信者の電子メール アドレスを選択してから[**次へ**]をクリックします。

3. [招待状の送信]ページが開いたら、[**完了**]をクリックします。

選択した Microsoft Outlook の電子メール アドレスを一覧表示した電子メールが自動生成されます。

4. テキストを編集し、自分の名前を署名します（オプション）。
5. [**送信**]をクリックします。

注記： Privacy Manager の証明書を取得していない場合、信頼済み連絡先要求の送信には Privacy Manager の証明書が必要というメッセージが表示されます。[**OK**]をクリックして、[証明書の要求ウィザード]を起動します。詳しくは、60 ページの「Privacy Manager の証明書の要求」を参照してください。

6. 選択したセキュリティ ログイン方法で認証します。

注記： 信頼済み連絡先の受信者は、電子メールを受信すると、電子メールを開いて右下隅の[**承認**]をクリックし、確認用のダイアログ ボックスが表示されたら[**OK**]をクリックする必要があります。

7. 信頼済み連絡先になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の[**承認**]をクリックします。

   ダイアログ ボックスが開き、受信者が信頼済み連絡先の一覧に正常に追加されたことを確認できます。

8. [**OK**]をクリックします。

信頼済み連絡先の詳細の表示

1. Privacy Manager を開き、[**信頼済み連絡先**]をクリックします。
2. 信頼済み連絡先をクリックします。
3. [**連絡先の詳細**]をクリックします。
4. 詳細の確認を終えたら、[**OK**]をクリックします。

信頼済み連絡先の削除

1. Privacy Manager を開き、[**信頼済み連絡先**]をクリックします。
2. 削除する信頼済み連絡先をクリックします。
3. [**連絡先の削除**]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

信頼済み連絡先の廃止状態の確認

信頼済み連絡先が自身の Privacy Manager の証明書を廃止しているかどうかを確認するには、以下の操作を行います。

1. Privacy Manager を開き、[**信頼済み連絡先**]をクリックします。
2. 信頼済み連絡先をクリックします。
3. [**詳細**]ボタンをクリックします。

   [高度な信頼済み連絡先管理]ダイアログ ボックスが開きます。

4. [**廃止の確認**]をクリックします。

5. [**閉じる**]をクリックします。

一般的なタスク

Privacy Manager は、以下の Microsoft 製品で使用できます。

- Microsoft Outlook
- Microsoft Office

[Microsoft Outlook]での Privacy Manager の使用

Privacy Manager をインストールすると、Microsoft Outlook のツールバーに[プライバシ]ボタンが表示されるようになります。また、Microsoft Outlook の各電子メール メッセージのツールバーに[安全に送信]ボタンが表示されるようになります。[**プライバシ**]または[**安全に送信**]の横にある下向き矢印をクリックすると、以下のオプションを選択できます。

- [**Sign and send message**]（メッセージに署名して送信）（[安全に送信]ボタンのみ）：このオプションを使用すると、電子メールにデジタル署名が付加されます。この電子メールは、選択したセキュリティ ログイン方法による認証の後に送信されます。
- [**Seal for Trusted Contacts and send message**]（メッセージを信頼済み連絡先宛てに封印して送信）（[安全に送信]ボタンのみ）：このオプションを使用すると、電子メールにデジタル署名が付加され、電子メールが暗号化されます。この電子メールは、選択したセキュリティ ログイン方法による認証の後に送信されます。
- [**連絡先の招待**]：このオプションを使用すると、信頼済み連絡先の招待状を送信できます。詳しくは、65 ページの「信頼済み連絡先の追加」を参照してください。
- [**Outlook のすべての連絡先を招待**]：このオプションを使用すると、Microsoft Outlook のアドレス帳に記載されているすべての連絡先に信頼済み連絡先の招待状を送信できます。詳しくは、65 ページの「Microsoft Outlook のアドレス帳を使用した信頼済み連絡先の追加」を参照してください。
- [**Privacy Manager ソフトウェアを開く**]：証明書、信頼済み連絡先、および[設定]オプションを使用すると、Privacy Manager ソフトウェアを開いて現在の設定の追加、表示、または変更ができます。詳しくは、60 ページの「Privacy Manager の証明書の管理」、64 ページの「信頼済み連絡先の管理」、または68 ページの「Microsoft Outlook 用の Privacy Manager の設定」を参照してください。

Microsoft Outlook 用の Privacy Manager の設定

1. Privacy Manager を開き、[**設定**]をクリックしてから[**電子メール**]タブをクリックします。

   または

   Microsoft Outlook のメインのツールバーで、[**安全に送信**]（Microsoft Outlook 2003 では[**プライバシ**]）の横にある下向きの矢印をクリックしてから[**設定**]をクリックします。

   または

   Microsoft の電子メール メッセージのツールバーで、[**安全に送信**]の横にある下向きの矢印をクリックしてから[**設定**]をクリックします。

2. 安全な電子メールを送信するときに実行する操作を選択し、[**OK**]をクリックします。

電子メール メッセージの署名および送信

1. Microsoft Outlook で、**[新規作成]** または **[返信]** をクリックします。
2. 電子メール メッセージを入力します。
3. **[安全に送信]**（Outlook 2003 の **[プライバシ]**）の横にある下向きの矢印をクリックしてから、**[署名して送信]** をクリックします。
4. 選択したセキュリティ ログイン方法で認証します。

電子メール メッセージの封印および送信

デジタル処理によって署名、封印（暗号化）されている、封印された電子メールを閲覧できるのは、信頼済み連絡先の一覧から選択したユーザーのみです。

電子メールを封印して信頼済み連絡先に送信するには、以下の操作を行います。

1. Microsoft Outlook で、**[新規作成]** または **[返信]** をクリックします。
2. 電子メール メッセージを入力します。
3. **[安全に送信]**（Outlook 2003 の **[プライバシ]**）の横にある下向きの矢印をクリックしてから、**[信頼済み連絡先宛てに封印して送信]** をクリックします。
4. 選択したセキュリティ ログイン方法で認証します。

封印された電子メール メッセージの表示

封印された電子メール メッセージを開くと、電子メールの見出しにセキュリティ ラベルが表示されます。このセキュリティ ラベルには、以下の情報が記載されています。

- 電子メールに署名した人物の身元確認に使用された証明書
- 電子メールに署名した人物の証明書の確認に使用された製品

Microsoft Office 2007 ドキュメントでの Privacy Manager の使用

Privacy Manager の証明書をインストールすると、Microsoft Word、Microsoft Excel、および Microsoft PowerPoint のすべてのドキュメントのツールバーの右側に、[署名と暗号化]ボタンが表示されます。**[署名と暗号化]** の横にある下向き矢印をクリックすると、以下のオプションを選択できます。

- **[ドキュメントへの署名]**：このオプションを使用すると、ドキュメントにデジタル署名が付加されます。
- **[署名の前に署名欄を追加]**（Microsoft Word および Microsoft Excel のみ）：初期設定では、Microsoft Word または Microsoft Excel のドキュメントに対する署名や暗号化が行われると、署名欄が追加されます。このオプションをオフにするには、**[署名欄の追加]** をクリックしてチェック マークを外します。
- **[ドキュメントの暗号化]**：このオプションを使用すると、ドキュメントにデジタル署名が付加され、ドキュメントが暗号化されます。
- **[暗号化の解除]**：このオプションを使用すると、ドキュメントの暗号化が解除されます。
- **[Privacy Manager ソフトウェアを開く]**：証明書、信頼済み連絡先、および[設定]オプションを使用すると、Privacy Manager ソフトウェアを開いて現在の設定の追加、表示、または変更ができます。詳しくは、60 ページの「Privacy Manager の証明書の管理」、64 ページの「信頼済み

連絡先の管理」、または70 ページの「Microsoft Office 用の Privacy Manager の設定」を参照してください。

Microsoft Office 用の Privacy Manager の設定

1. Privacy Manager を開き、[**設定**]をクリックしてから[**ドキュメント**]タブをクリックします。

   または

   Microsoft Office ドキュメントのツールバーで、[**署名と暗号化**]の横にある下向きの矢印をクリックしてから[**設定**]をクリックします。

2. 設定する操作を選択し、[**OK**]をクリックします。

Microsoft Office ドキュメントへの署名

1. Microsoft Word、Microsoft Excel、または Microsoft PowerPoint でドキュメントを作成し、保存します。
2. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**ドキュメントへの署名**]をクリックします。
3. 選択したセキュリティ ログイン方法で認証します。
4. 確認用のダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから[**OK**]をクリックします。

後でドキュメントを編集する場合は、以下の操作を行います。

1. 画面の左上隅にある[**Office**]ボタンをクリックします。
2. [**準備**]→[**最終版としてマーク**]の順にクリックします。
3. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックして作業を続けます。
4. 編集が終わったら、再びドキュメントに署名します。

Microsoft Word または Microsoft Excel ドキュメント署名時の署名欄の追加

Privacy Manager では、Microsoft Word または Microsoft Excel ドキュメントに署名する場合に署名欄を追加できます。

1. Microsoft Word または Microsoft Excel でドキュメントを作成し、保存します。
2. [**ホーム**]メニューをクリックします。
3. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**署名の前に署名欄を追加**]をクリックします。

   注記： このオプションを選択すると、[署名の前に署名欄を追加]の横にチェック マークが表示されます。初期設定では、このオプションは有効になっています。

4. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**ドキュメントへの署名**]をクリックします。
5. 選択したセキュリティ ログイン方法で認証します。

Microsoft Word または Microsoft Excel ドキュメントに、推奨する署名者を追加する

推奨する署名者を指名することによって、ドキュメントに複数の署名欄を追加できます。推奨する署名者とは、ドキュメントに署名欄を追加するために Microsoft Word または Microsoft Excel ドキュメントの所有者が指名したユーザーのことです。推奨する署名者には自分自身を指名することも、別の人物を指名してドキュメントへの署名を依頼することもできます。たとえば、部署内の全員の署名が必要なドキュメントを準備する場合、特定の日付で署名するよう指示した全員分の署名欄を、ドキュメントの最終ページの最下部に設けることができます。

Microsoft Word または Microsoft Excel ドキュメントに、推奨する署名者を追加するには、以下の操作を行います。

1. Microsoft Word または Microsoft Excel でドキュメントを作成し、保存します。
2. [**挿入**]メニューをクリックします。
3. ツールバーの[**テキスト**]グループで、[**署名欄**]の横にある矢印をクリックしてから[**Privacy Manager 署名プロバイダー**]をクリックします。

   [署名の設定]ダイアログ ボックスが表示されます。
4. ボックス内の[**推奨する署名者**]の下に、推奨する署名者の名前を入力します。
5. ボックス内の[**署名者への指示**]の下に、この推奨する署名者へのメッセージを入力します。

   注記： このメッセージはタイトルとして表示されますが、ドキュメントに署名すると、削除したりユーザーのタイトルに置き換えたりすることができます。
6. [**署名欄に署名日を表示**]チェック ボックスにチェックを入れて、日付を表示します。
7. [**署名欄に署名者のタイトルを表示**]チェック ボックスにチェックを入れて、タイトルを表示します。

   注記： ドキュメントの所有者は、推奨する署名者を自身のドキュメントに割り当てます。推奨する署名者が署名欄に日付やタイトルを表示できるようにするには、[**署名欄に署名日を表示**]および[**署名欄に署名のタイトルを表示**]の各チェック ボックスにチェックが入っている必要があります。
8. [**OK**]をクリックします。

推奨する署名者の署名欄の追加

推奨する署名者がドキュメントを開くと、自分の名前が角かっこで囲まれて表示され、署名を求められていることがわかります。

ドキュメントに署名するには、以下の操作を行います。

1. 適切な署名欄をダブルクリックします。
2. 選択したセキュリティ ログイン方法で認証します。

   ドキュメントの所有者が指定した設定に従って、署名欄が表示されます。

Microsoft Office ドキュメントの暗号化

ユーザーおよび信頼済み連絡先が使用する Microsoft Office ドキュメントを暗号化できます。ドキュメントを暗号化してから閉じると、ユーザーおよびユーザーが一覧から選択した信頼済み連絡先は、このドキュメントを開くときに認証が必要となります。

Microsoft Office ドキュメントを暗号化するには、以下の操作を行います。

1. Microsoft Word、Microsoft Excel、または Microsoft PowerPoint でドキュメントを作成し、保存します。
2. [**ホーム**]メニューをクリックします。
3. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**ドキュメントの暗号化**]をクリックします。

   [信頼済み連絡先の選択]ダイアログ ボックスが表示されます。
4. ドキュメントを開いて内容を閲覧できるようにする信頼済み連絡先の名前をクリックします。

   注記： 信頼済み連絡先の名前を複数選択するには、ctrl キーを押しながら個々の名前をクリックします。
5. [**OK**]をクリックします。

後でドキュメントを編集する場合は、72 ページの「Microsoft Office ドキュメントの暗号化の解除」に記載されている操作を行います。暗号化を解除すると、ドキュメントを編集できます。再びドキュメントを暗号化するには、ここに記載されている操作を行います。

Microsoft Office ドキュメントの暗号化の解除

Microsoft Office ドキュメントの暗号化を解除すると、ユーザーおよび信頼済み連絡先は、認証なしでこのドキュメントを開いて内容を閲覧できるようになります。

Microsoft Office ドキュメントの暗号化を解除するには、以下の操作を行います。

1. 暗号化された Microsoft Word、Microsoft Excel、または Microsoft PowerPoint ドキュメントを開きます。
2. 選択したセキュリティ ログイン方法で認証します。
3. [**ホーム**]メニューをクリックします。
4. [**署名と暗号化**]の横にある下向きの矢印をクリックしてから、[**暗号化の解除**]をクリックします。

暗号化された Microsoft Office ドキュメントの送信

電子メール メッセージに、暗号化された Microsoft Office ドキュメントを添付できます。電子メール自体への署名や暗号化は不要です。これには、ファイルを添付した一般の電子メールの場合と同様に、署名または暗号化したドキュメントを添付した電子メールを作成し、送信します。

ただし、最適なセキュリティのため、署名または暗号化された Microsoft Office ドキュメントを添付する場合には、電子メールを暗号化することをおすすめします。

署名および暗号化した Microsoft Office ドキュメントを添付して、封印した電子メールを送信するには、以下の操作を行います。

1. Microsoft Outlook で、[**新規作成**]または[**返信**]をクリックします。
2. 電子メール メッセージを入力します。

3. Microsoft Office ドキュメントを添付します。

4. 詳しい手順については、69 ページの「電子メール メッセージの封印および送信」を参照してください。

署名付き Microsoft Office ドキュメントの表示

注記： 署名付き Microsoft Office ドキュメントを表示するには、Privacy Manager の証明書は不要です。

署名付き Microsoft Office ドキュメントを開くと、ドキュメント ウィンドウ下部のステータス バーに[デジタル署名]アイコンが表示されます。

1. [**デジタル署名**]アイコンをクリックすると、[署名]ダイアログ ボックスの表示が切り替わります。このダイアログには、ドキュメントに署名したすべてのユーザー名とその個々の署名日が表示されます。

2. 個々の署名の詳細を表示するには、[署名]ダイアログ ボックスで名前を右クリックして[**署名の詳細**]を選択します。

暗号化された Microsoft Office ドキュメントの表示

暗号化された Microsoft Office ドキュメントを別のコンピューターから閲覧するには、そのコンピューターに Privacy Manager をインストールしておく必要があります。ファイルの暗号化に使用した Privacy Manager の証明書を復元する必要もあります。

証明書が失われてしまっている場合、暗号化された Microsoft Office ドキュメントを表示するには、ファイルを暗号化するときに使用された Privacy Manager の証明書を復元する必要があります。

信頼済み連絡先が暗号化された Microsoft Office ドキュメントを閲覧するには、Privacy Manager の証明書が必要です。なお、コンピューターに Privacy Manager をインストールしておく必要があります。また、暗号化された Microsoft Office ドキュメントの所有者が、この信頼済み連絡先を選択している必要があります。

高度なタスク

別のコンピューターへの Privacy Manager Certificate と信頼済み連絡先の移行

Privacy Manager の証明書および信頼済み連絡先を、安全に別のコンピューターに移行したり、安全にデータをバックアップしたりできます。これには、ネットワーク上またはリムーバル ストレージデバイスに、パスワードで保護されたファイルとして Privacy Manager の証明書および信頼済み連絡先のバックアップを作成してから、新しいコンピューターにこのファイルを復元します。

Privacy Manager の証明書および信頼済み連絡先のバックアップ

Privacy Manager の証明書および信頼済み連絡先をパスワードで保護されたファイルにバックアップするには、以下の操作を行います。

1. Privacy Manager を開き、[**移行**]をクリックします。
2. [**バックアップ**]をクリックします。
3. [データの選択]ページで、移行ファイルに含めるデータのカテゴリを選択してから[**次へ**]をクリックします。
4. [移行ファイル]ページで、ファイル名を入力するか、[**参照**]をクリックして場所を探し、[**次へ**]をクリックします。
5. パスワードの入力と確認を行い、[**次へ**]をクリックします。

注記： 移行ファイルを復元するときに必要ですので、このパスワードは安全な場所に保管してください。

6. 選択したセキュリティ ログイン方法で認証します。
7. [移行ファイルを保存しました]ページで、[**完了**]をクリックします。

Privacy Manager の証明書および信頼済み連絡先の復元

別のコンピューター上での移行プロセスの一つとして、または同じコンピューター上で Privacy Manager の証明書および信頼済み連絡先を復元するには、以下の操作を行います。

1. Privacy Manager を開き、[**移行**]をクリックします。
2. [**復元**]をクリックします。
3. [移行ファイル]ページで[**参照**]をクリックしてファイルを探し、[**次へ**]をクリックします。
4. バックアップ ファイル作成時に使用したパスワードを入力して、[**次へ**]をクリックします。
5. [移行ファイル]ページで、[**完了**]をクリックします。

Privacy Manager の集中管理

お使いの Privacy Manager は、集中管理でインストールされ、管理者によって機能や設定がカスタマイズされているものである場合があります。以下の機能のうち 1 つ以上が、有効または無効にされている可能性があります。

- **証明書使用ポリシー**：証明書の使用は、Comodo によって発行される Privacy Manager 証明書に限定される場合があります。または、その他の証明機関によって発行されるデジタル証明書のみの使用が許可される場合があります。
- **暗号化ポリシー**：暗号化機能は、Microsoft Office または Microsoft Outlook で、個別に有効または無効に設定されている可能性があります。

7 File Sanitizer for HP ProtectTools

File Sanitizer を使用すると、コンピューター上のフォルダーやファイル（例：個人情報やファイル、履歴データや Web 関連データ、その他のデータ コンポーネント）を安全にシュレッドしたり、ハードドライブ上の削除されたフォルダーやファイルを定期的にブリーチ（漂白）したりすることができます。

注記： このバージョンの File Sanitizer は、コンピューターのハードドライブのみをサポートしています。

シュレッド

シュレッドは、通常の Windows の削除（File Sanitizer ではシンプル削除とも呼ばれます）とは異なります。File Sanitizer を使用してフォルダーやファイルをシュレッドすると、ファイルに意味を持たないデータが上書きされて、元のフォルダーやファイルを取り戻すことが事実上不可能になります。Windows のシンプル削除では、ファイル（またはフォルダー）がハードドライブ上にそのままの状態で残されるか、または電子情報の分析によって復元できる状態で残される可能性があります。

シュレッド プロファイル（[**セキュリティ設定、高**]、[**セキュリティ設定、中**]、または[**セキュリティ設定、低**]）を選択すると、あらかじめ定義されているフォルダーやファイルの一覧と消去方法がシュレッドのために自動で選択されます。また、シュレッド プロファイルをカスタマイズして、シュレッド サイクル数、シュレッド対象に含めるフォルダーやファイル、シュレッド前に確認するフォルダーやファイル、およびシュレッド対象から除外するフォルダーやファイルを指定することもできます。詳しくは、81 ページの「シュレッド プロファイルの選択または作成」を参照してください。

タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを使用して、自動シュレッドのスケジュールを設定するか、シュレッドを手動で実行できます。詳しくは、80 ページの「シュレッド スケジュールの設定」、85 ページの「単一フォルダーやファイルの手動シュレッド」、または 85 ページの「選択されているすべてのフォルダーやファイルの手動シュレッド」を参照してください。

注記： .dll ファイルは、ゴミ箱に移動されている場合にのみ、シュレッドされてシステムから削除されます。

空き領域ブリーチ

Windows でフォルダーやファイルを削除しても、その内容はハードドライブから完全に削除されません。Windows はフォルダーやファイルの参照情報のみを削除します。他のフォルダーやファイルによってハードドライブの同じ領域を新しい情報で上書きしないかぎり、フォルダーやファイルの内容はハードドライブに引き続き残ったままとなります。

空き領域ブリーチを実行すると、削除されたフォルダーやファイルに対してランダムなデータを安全に上書きできるため、削除されたフォルダーやファイルの元の内容をユーザーは参照できなくなります。

注記： 空き領域ブリーチは、File Sanitizer の[**シンプル削除の設定**]を選択したり Windows のゴミ箱に移動したりして削除したフォルダーやファイル、または手動で削除したフォルダーやファイルを対象として随時実行できます。空き領域ブリーチを実行しても、シュレッドされたフォルダーやファイルにセキュリティが追加されることはありません。

タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを使用して、空き領域ブリーチの自動スケジュールを有効にするか、空き領域ブリーチを手動で実行できます。詳しくは、80 ページの「空き領域ブリーチのスケジュール設定」、または86 ページの「空き領域ブリーチの手動実行」を参照してください。

File Sanitizer の起動

1. [**スタート**]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools Security Manager**]の順にクリックします。
2. [**File Sanitizer**]をクリックします。

または

▲ デスクトップにある[**File Sanitizer**]アイコンをダブルクリックします。

または

▲ タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックしてから、[**File Sanitizer**]→[**File Sanitizer を開く**]の順にクリックします。

セットアップ手順

シュレッド スケジュールの設定

あらかじめ定義されているシュレッド プロファイルを選択したり、独自のシュレッド プロファイルを作成したりできます。詳しくは、81 ページの「シュレッド プロファイルの選択または作成」を参照してください。フォルダーやファイルは、いつでも手動シュレッドできます。詳しくは、84 ページの「キーの組み合わせによるシュレッドの開始」を参照してください。

注記： スケジュールされたタスクは特定の時刻に開始します。スケジュール設定した時刻にシステムの電源が切れているか、スリープ/スタンバイ状態になっているときは、File Sanitizer はタスクの再起動を試みません。

1. File Sanitizer を起動して、[**シュレッド**]をクリックします。
2. 以下の中から 1 つ以上のシュレッド オプションを選択します。
   - [**Windows のシャットダウン時**]：選択されているすべてのフォルダーやファイルを Windows のシャットダウン時にシュレッドします。

     注記： シャットダウン時にダイアログ ボックスが表示され、選択されているフォルダーやファイルのシュレッドを実行するか、シュレッド処理を中止するかを確認します。

     シュレッド処理を中止する場合は[**はい**]、シュレッドを実行する場合は[**いいえ**]をクリックします。
   - [**Web ブラウザーの起動時**]：ブラウザーの URL 履歴など、選択されているすべての Web 関連フォルダーやファイルを Web ブラウザーの起動時にシュレッドします。
   - [**Web ブラウザーの終了時**]：ブラウザーの URL 履歴など、選択されているすべての Web 関連フォルダーやファイルを Web ブラウザーの終了時にシュレッドします。
   - [**キーの組み合わせ**]：シュレッドを開始するためのキーの組み合わせを指定できます。詳しくは、84 ページの「キーの組み合わせによるシュレッドの開始」を参照してください。

   注記： .dll ファイルは、ゴミ箱に移動されている場合にのみ、シュレッドされてシステムから削除されます。
3. 選択されているフォルダーやファイルを将来のある時点にシュレッドするようにスケジュール設定するには、[**スケジューラの起動**]チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、日付と時刻を選択します。
4. [**適用**]をクリックします。

空き領域ブリーチのスケジュール設定

空き領域ブリーチは、File Sanitizer の[**シンプル削除の設定**]を選択したり Windows のゴミ箱に移動したりして削除したフォルダーやファイル、または手動で削除したフォルダーやファイルを対象として随時実行できます。空き領域ブリーチを実行しても、シュレッドされたフォルダーやファイルにセキュリティが追加されることはありません。

注記： スケジュールされたタスクは特定の時刻に開始します。スケジュール設定した時刻にシステムの電源が切れているか、スリープ/スタンバイ状態になっているときは、File Sanitizer はタスクの再起動を試みません。

1. File Sanitizer を起動して、[**ブリーチ**]をクリックします。
2. 将来のある時点にハードドライブ上の削除されたフォルダーやファイルをブリーチするようにスケジュール設定するには、[**スケジューラの起動**]チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、日付と時刻を選択します。
3. [**適用**]をクリックします。

注記： 空き領域ブリーチ操作は、非常に長い時間がかかる場合があります。空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。

シュレッド プロファイルの選択または作成

あらかじめ定義されているプロファイルを選択するか、自分のプロファイルを作成して、消去方法を指定したりシュレッドするフォルダーやファイルを選択したりできます。

あらかじめ定義されているシュレッド プロファイルの選択

あらかじめ定義されているシュレッド プロファイルを選択すると、あらかじめ定義されている消去方法とフォルダーやファイルの一覧が自動的に選択されます。シュレッド用に選択されているフォルダーやファイルのあらかじめ定義されている一覧を表示することもできます。

1. File Sanitizer を起動し、[**設定**]をクリックします。
2. あらかじめ定義されているシュレッド プロファイルをクリックします。
   - [**セキュリティ設定、高**]
   - [**セキュリティ設定、中**]
   - [**セキュリティ設定、低**]
3. シュレッド用に選択されているフォルダーやファイルを表示するには、[**詳細を表示**]をクリックします。
   a. [**選択した項目はシュレッドされ、確認メッセージが表示されます。選択していない項目はシュレッドされますが、確認メッセージは表示されません。**]：項目をシュレッドする前に確認メッセージを表示するには、チェック ボックスにチェックを入れます。確認メッセージを表示しないで項目をシュレッドするには、チェック ボックスのチェックを外します。

      注記： 項目のチェック ボックスのチェックを外しても、その項目はシュレッドされます。

   b. [**適用**]をクリックします。
4. [**適用**]をクリックします。

シュレッド プロファイルのカスタマイズ

シュレッド プロファイルを作成するには、シュレッド サイクル数、シュレッド対象に含めるフォルダーやファイル、シュレッド前に確認するフォルダーやファイル、およびシュレッド対象から除外するフォルダーやファイルを指定します。

1. File Sanitizer を起動し、[**設定**]→[**高度なセキュリティ設定**]→[**詳細を表示**]の順にクリックします。
2. シュレッド サイクル数を選択します。

   注記： 各フォルダーやファイルに対して、指定した数のシュレッド サイクルが実行されます。たとえば、シュレッド サイクルで[3]を選択すると、データの内容をわからなくするアルゴリズムが 3 つの別々の時間に実行されます。高いセキュリティ設定でシュレッド サイクルを選択すると、シュレッドに非常に長い時間がかかる場合があります。ただし、指定するシュレッド サイクル数を大きくするほど、データを取得できる可能性は低くなります。

3. 以下の要領で、シュレッド対象のフォルダーやファイルを選択します。

   a. [**使用できるシュレッド オプション**]で、フォルダーやファイルをクリックしてから[**追加**]をクリックします。

   b. カスタム フォルダーやファイルを追加するには、[**カスタム オプションの追加**]をクリックし、フォルダーやファイルのパスを選択または入力します。

   c. [**開く**]→[**OK**]の順にクリックします。

   d. [**使用できるシュレッド オプション**]で、追加するフォルダーやファイルをクリックしてから[**追加**]をクリックします。

   [使用できるシュレッド オプション]からフォルダーやファイルを削除するには、削除するフォルダーやファイルをクリックしてから[**削除**]をクリックします。

4. [**選択した項目はシュレッドされ、確認メッセージが表示されます。選択していない項目はシュレッドされますが、確認メッセージは表示されません。**]：項目をシュレッドする前に確認メッセージを表示するには、チェック ボックスにチェックを入れます。確認メッセージを表示しないで項目をシュレッドするには、チェック ボックスのチェックを外します。

   注記： 項目のチェック ボックスのチェックを外しても、その項目はシュレッドされます。

   シュレッド リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから[**削除**]をクリックします。

5. 自動シュレッドからフォルダーやファイルを保護するには、以下の操作を行います。

   a. [**次のフォルダー/ファイルをシュレッドしない**]で[**追加**]をクリックし、フォルダーやファイルのパスを選択または入力します。

   b. [**開く**]→[**OK**]の順にクリックします。

   除外リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから[**削除**]をクリックします。

6. [**適用**]をクリックします。

シンプル削除プロファイルのカスタマイズ

シンプル削除プロファイルは、シュレッドしないで標準的なフォルダーやファイルの削除を実行します。また、シンプル削除プロファイルをカスタマイズして、シンプル削除対象に含めるフォルダーやファイル、シンプル削除の実行前に確認するフォルダーやファイル、およびシンプル削除対象から除外するフォルダーやファイルを指定できます。

注記： ［**シンプル削除の設定**］を選択する場合は、手動で削除したフォルダーやファイル、またはWindwos のゴミ箱を使用して削除されたフォルダーやファイルに空き領域ブリーチを随時実行できます。

1. File Sanitizer を起動し、［**設定**］→［**シンプル削除の設定**］→［**詳細を表示**］の順にクリックします。

2. 削除するフォルダーやファイルを選択するには、以下の操作を行います。

   a. ［**使用できる削除オプション**］で、フォルダーやファイルをクリックしてから［**追加**］をクリックします。

   b. カスタム フォルダーやファイルを追加するには、［**カスタム オプションの追加**］をクリックし、フォルダーやファイルのパスを選択または入力して、［**OK**］をクリックします。

   c. カスタム フォルダーやファイルをクリックして、［**追加**］をクリックします。

   使用できる削除オプションからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから［**削除**］をクリックします。

3. ［**選択した項目はシュレッドされ、確認メッセージが表示されます。選択していない項目はシュレッドされますが、確認メッセージは表示されません。**］：項目をシュレッドする前に確認メッセージを表示するには、チェック ボックスにチェックを入れます。確認メッセージを表示しないで項目をシュレッドするには、チェック ボックスのチェックを外します。

   注記： 項目のチェック ボックスのチェックを外しても、その項目はシュレッドされます。

   削除リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから［**削除**］をクリックします。

4. 自動削除からフォルダーやファイルを保護するには、以下の操作を行います。

   a. ［**次のフォルダー/ファイルを削除しない**］で［**追加**］をクリックし、フォルダーやファイルのパスを選択または入力します。

   b. ［**開く**］→［**OK**］の順にクリックします。

   除外リストからフォルダーやファイルを削除するには、フォルダーやファイルをクリックしてから［**削除**］をクリックします。

5. ［**適用**］をクリックします。

一般的なタスク

File Sanitizer を使用すると、以下のタスクを実行できます。

- キーの組み合わせでシュレッドを開始：この機能によって、（たとえば、ctrl ＋ alt ＋ delete などの）キーの組み合わせを作成してシュレッドを開始できます。詳しくは、84 ページの「キーの組み合わせによるシュレッドの開始」を参照してください。
- [File Sanitizer]アイコンでシュレッドを開始：これは、Windows のドラッグ アンド ドロップと同様の機能です。詳しくは、85 ページの「[File Sanitizer]アイコンの使用」を参照してください。
- 特定のフォルダーやファイルまたは選択されているすべてのフォルダーやファイルを手動シュレッド：この機能によって、通常のシュレッド スケジュールの実行前に、手動でフォルダーやファイルをシュレッドできます。詳しくは、85 ページの「単一フォルダーやファイルの手動シュレッド」または85 ページの「選択されているすべてのフォルダーやファイルの手動シュレッド」を参照してください。
- 空き領域ブリーチを手動で実行：この機能によって、空き領域ブリーチを手動で実行できます。詳しくは、86 ページの「空き領域ブリーチの手動実行」を参照してください。
- シュレッド操作または空き領域ブリーチ操作を停止：この機能によって、シュレッド操作または空き領域ブリーチ操作を停止できます。詳しくは、86 ページの「シュレッド操作または空き領域ブリーチ操作の停止」を参照してください。
- ログ ファイルを表示：この機能によって、シュレッドまたは空き領域ブリーチのログ ファイルを表示できます。ログ ファイルには、最後のシュレッド操作または空き領域操作で発生したエラーや障害が記録されます。詳しくは、86 ページの「ログ ファイルの表示」を参照してください。

注記：　シュレッド操作または空き領域ブリーチ操作は、非常に長い時間がかかる場合があります。シュレッドや空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。

キーの組み合わせによるシュレッドの開始

1. File Sanitizer を起動して、[**シュレッド**]をクリックします。
2. [**キーの組み合わせ**]チェック ボックスにチェックを入れます。
3. 使用できるボックスに文字を 1 つ入力します。
4. [**CTRL**]ボックスまたは[**ALT**]ボックスのどちらかを選択してから[**SHIFT**]ボックスを選択します。

   たとえば、s キーと ctrl ＋ shift キーを使用して自動シュレッドを開始するには、ボックスに s と入力してから、[**CTRL**]オプションと[**SHIFT**]オプションにチェックを入れます。

   注記：　設定済みの他のキーの組み合わせとは異なるキーの組み合わせを選択してください。

キーの組み合わせでシュレッドを開始するには、以下の操作を行います。

1. shift キーと ctrl キーまたは alt キー（または指定した組み合わせのキー）を押しながら、選択した文字キーを押します。
2. 確認用のダイアログ ボックスが表示されたら、[**はい**]をクリックします。

[File Sanitizer]アイコンの使用

⚠ **注意：** シュレッドしたフォルダーやファイルは復元できません。手動でシュレッドするために選択するフォルダーやファイルについては、十分に検討してください。

1. シュレッドするドキュメントまたはフォルダーに移動します。
2. シュレッドするフォルダーやファイルをデスクトップの[**File Sanitizer**]アイコンにドラッグします。
3. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

単一フォルダーやファイルの手動シュレッド

⚠ **注意：** シュレッドしたフォルダーやファイルは復元できません。手動でシュレッドするために選択するフォルダーやファイルについては、十分に検討してください。

1. タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックしてから、[**File Sanitizer**]→[**単一フォルダー/ファイルをシュレッド**]の順にクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルに移動してから[**OK**]をクリックします。

   注記： 選択できるフォルダーやファイルは、単一のファイルまたはフォルダーです。

3. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

または

1. デスクトップにある[**File Sanitizer**]アイコンを右クリックしてから、[**単一フォルダー/ファイルをシュレッド**]をクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルに移動してから[**OK**]をクリックします。
3. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

または

1. File Sanitizer を起動して、[**シュレッド**]をクリックします。
2. [**参照**]ボタンをクリックします。
3. [参照]ダイアログ ボックスが開いたら、シュレッドするフォルダーやファイルに移動してから[**OK**]をクリックします。
4. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

選択されているすべてのフォルダーやファイルの手動シュレッド

1. タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックしてから、[**File Sanitizer**]→[**今すぐシュレッド**]の順にクリックします。
2. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

または

1. デスクトップにある[**File Sanitizer**]アイコンを右クリックしてから、[**今すぐシュレッド**]をクリックします。
2. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

または

1. File Sanitizer を起動して、[**シュレッド**]をクリックします。
2. [**今すぐシュレッド**]ボタンをクリックします。
3. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

空き領域ブリーチの手動実行

1. タスクバーの右端の通知領域にある[**HP ProtectTools**]アイコンを右クリックしてから、[**File Sanitizer**]→[**今すぐブリーチ**]の順にクリックします。
2. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

または

1. File Sanitizer を起動して、[**空き領域ブリーチ**]をクリックします。
2. [**今すぐブリーチ**]をクリックします。
3. 確認用のダイアログ ボックスが開いたら、[**はい**]をクリックします。

シュレッド操作または空き領域ブリーチ操作の停止

シュレッド操作または空き領域ブリーチ操作の実行中、タスクバーの右端の通知領域にある[HP ProtectTools Security Manager]アイコンの上にメッセージが表示されます。このメッセージには、シュレッド処理または空き領域ブリーチ処理の詳細（完了した割合）と、操作を停止するためのオプションが表示されます。

▲ 操作をキャンセルするには、メッセージをクリックしてから[**停止**]をクリックします。

ログ ファイルの表示

シュレッド操作または空き領域ブリーチ操作を実行するたびに、エラーのログ ファイルまたは障害のログ ファイルが生成されます。これらのログ ファイルは、最新のシュレッド操作または空き領域ブリーチ操作に従って常に更新されます。

注記： 正常にシュレッドまたはブリーチされたファイルは、ログ ファイルには表示されません。

ログ ファイルには、シュレッド操作について作成されるファイルと空き領域ブリーチ操作について作成されるファイルがあります。これらのログ ファイルは、ハードドライブ上の以下の場所にあります。

- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥**[ユーザー名]**_ShredderLog.txt
- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥**[ユーザー名]**_DiskBleachLog.txt

64 ビットのシステムでは、これらのログ ファイルは、ハードドライブ上の以下の場所にあります。

- C:¥Program Files (x86)¥Hewlett-Packard¥File Sanitizer¥**[ユーザー名]**_ShredderLog.txt
- C:¥Program Files (x86)¥Hewlett-Packard¥File Sanitizer¥**[ユーザー名]**_DiskBleachLog.txt

8　Device Access Manager for HP ProtectTools（一部のモデルのみ）

HP ProtectTools Device Access Manager は、データ転送デバイスを無効にすることによってデータへのアクセスを制御します。

注記：　マウス、キーボード、タッチパッド、指紋認証システムなどの一部のヒューマン インターフェイス デバイスや入力デバイスは、Device Access Manager によって制御されません。詳しくは、99 ページの「管理されないデバイス クラス」を参照してください。

HP ProtectTools Device Access Manager を使用すると、Windows オペレーティング システムの管理者は、システム上のデバイスへのアクセスを制御し、不正なアクセスを防止できます。

- アクセスを許可または拒否するデバイスを定義するためのデバイス プロファイルが、ユーザーごとに作成されます。
- ジャスト イン タイム認証（JITA）を使用すると、あらかじめ定義されたユーザーは、通常はアクセスできないデバイスにアクセスするために、自身を認証することが可能です。
- 管理者および信頼できるユーザーをデバイス管理グループに追加することで、[Device Access Manager]によるデバイスへのアクセス制限からこれらの管理者やユーザーを除外できます。このグループのメンバーシップは、[詳細設定]を使用して管理します。
- グループ メンバーシップに基づいて、または個々のユーザーに対して、デバイス アクセスを許可または拒否できます。
- CD-ROM ドライブや DVD ドライブなどのデバイス クラスの場合は、読み取りアクセスおよび書き込みアクセスを個別に許可または拒否できます。

Device Access Manager を開く

1. 管理者としてログインします。
2. [スタート]→[**すべてのプログラム**]→[**HP**]→[**HP ProtectTools 管理者コンソール**]の順にクリックします。
3. 左側の枠内で、[**Device Access Manager**]をクリックします。

ユーザーは、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）を使用して HP ProtectTools Device Access Manager ポリシーを表示できます。このコンソールのビューは読み取り専用です。

セットアップ手順

デバイス アクセスの設定

HP ProtectTools Device Access Manager には、以下の 4 つのビューがあります。

- **[簡易構成]**：デバイス管理者グループのメンバーシップに基づいて、デバイス クラスへのアクセスを許可または拒否します。
- **[デバイス クラス構成]**：特定のユーザーまたはグループに対して、特定の種類のデバイスまたは特定のデバイスへのアクセスを許可または拒否します。
- **[ジャスト イン タイム認証の構成]**：選択されたユーザーが自身を認証して DVD デバイスや CD-ROM デバイスまたはリムーバブル メディアにアクセスできるようにする、ジャスト イン タイム認証（JITA）を構成します。
- **[詳細設定]**：C ドライブ、システム ドライブなど、Device Access Manager によってアクセスを制限されないドライブ文字の一覧を構成します。デバイス管理者グループのメンバーシップもこのビューから管理できます。

簡易構成

管理者は、**[簡易構成]**ビューを使用して、デバイス管理者以外のすべてのユーザーによる以下のデバイス クラスへのアクセスを許可または拒否できます。

- すべてのリムーバブル メディア（フロッピーディスク、USB フラッシュ ドライブなど）
- すべての DVD/CD-ROM ドライブ
- すべてのシリアル コネクタおよびパラレル コネクタ
- すべての Bluetooth デバイス
- すべてのモデム デバイス
- すべての PCMCIA/ExpressCard デバイス
- すべての 1394 デバイス

デバイス管理者以外のすべてのユーザーによるデバイス クラスへのアクセスを許可または拒否するには、以下の操作を行います。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、**[Device Access Manager]**→**[簡易構成]**の順にクリックします。
2. アクセスを拒否するには、右側の枠内で、デバイス クラスまたは特定のデバイスのチェック ボックスにチェックを入れます。アクセスを許可するには、デバイス クラスまたは特定のデバイスのチェックボックスのチェックを外します。

   チェック ボックスがグレーで表示されている場合は、アクセス方法に影響を与える値が**[デバイス クラス構成]**ビューで変更されています。工場出荷時の設定に戻すには、**[デバイス クラス構成]**ビューで**[リセット]**をクリックします。
3. **[適用]**をクリックします。

注記： バックグラウンド サービスが実行されていない場合は、サービスを開始するかどうかを尋ねるダイアログ ボックスが表示されます。[**はい**]をクリックします。

4. [**OK**]をクリックします。

バックグラウンド サービスの開始

新しいポリシーが初めて定義されて適用されると、[HP ProtectTools デバイス ロック/検査]バックグラウンド サービスが自動的に開始され、システムが起動するたびに自動的に開始するように設定されます。

注記： バックグラウンド サービスの開始を尋ねる画面が表示される前に、デバイス プロファイルを定義しておく必要があります。

管理者は、以下の操作を行うことでもサービスを開始または停止できます。

1. Windows 7 をお使いの場合は、[**スタート**]→[**コントロール パネル**]→[**システムとセキュリティ**]の順にクリックします。

   または

   Windows Vista®をお使いの場合は、[**スタート**]→[**コントロール パネル**]→[**システムとメンテナンス**]の順にクリックします。

   または

   Windows XP をお使いの場合は、[**スタート**]→[**コントロール パネル**]→[**パフォーマンスとメンテナンス**]の順にクリックします。

2. [**管理ツール**]→[**サービス**]の順にクリックします。
3. [**HP ProtectTools デバイス ロック/検査**]サービスを検索して設定します。
4. サービスを開始するには、[**開始**]をクリックします。

   または

   実行されているサービスを停止するには、[**停止**]をクリックします。

[HP ProtectTools デバイス ロック/検査]サービスを停止しても、デバイス ロックは停止されません。デバイス ロックは、以下の 2 つのコンポーネントによって実行されています。

- [HP ProtectTools デバイス ロック/検査]サービス
- DAMDrv.sys ドライバー

サービスを開始するとこのデバイス ドライバーが開始されますが、サービスを停止してもこのドライバーは停止されません。

このバックグラウンド サービスが実行されているかどうかを確認するには、コマンド プロンプト ウィンドウを開いて「sc query flcdlock」と入力します。

このデバイス ドライバーが実行されているかどうかを確認するには、コマンド プロンプト ウィンドウを開いて「sc query damdrv」と入力します。

デバイス クラス構成

管理者は、デバイス クラスまたは特定のデバイスへのアクセスを許可または拒否されているユーザーおよびグループを一覧から表示したり編集したりできます。

[**デバイス クラス構成**]ビューには以下のセクションがあります。

- [**デバイス一覧**]：デバイス クラス、およびシステムにインストールされているか以前にインストールされていた可能性のあるデバイスをすべて表示します。
  - 保護は、通常はデバイス クラスに対して適用されます。選択されたユーザーまたはグループは、そのデバイス クラスの任意のデバイスにアクセスできます。
  - 特定のデバイスに対して保護を適用することもできます。
- [**ユーザー一覧**]：選択されたデバイス クラスまたは特定のデバイスへのアクセスを許可または拒否されているユーザーおよびグループをすべて表示します。
  - [ユーザー一覧]には、特定のユーザーまたはそのユーザーがメンバーとなっているグループを登録できます。
  - [ユーザー一覧]でユーザーまたはグループを利用できない場合は、設定が[デバイス一覧]のデバイス クラスまたは[クラス]フォルダーから継承されています。
  - DVD や CD-ROM など一部のデバイス クラスでは、読み取りおよび書き込み操作のためのアクセスを個別に許可または拒否することによって詳細な制御を設定できます。

    それ以外のデバイスおよびクラスでは、読み取りおよび書き込みアクセス権を継承できます。たとえば、読み取りアクセス権は上位のクラスから継承し、書き込みアクセス権はユーザーまたはグループごとに定義するといった設定が可能です。

    注記： [**読み取り**]チェック ボックスのチェックが外れている場合、アクセス制御の登録内容はデバイスへの読み取りアクセスに影響を与えませんが、読み取りアクセスが拒否されるわけではありません。

    注記： Administrators グループを[ユーザー一覧]に追加することはできません。代わりに、デバイス管理者グループを使用します。

    例 1：ユーザーまたはグループがデバイスまたはデバイス クラスへの書き込みアクセスを拒否されている場合

    このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを許可できます。

    例 2：ユーザーまたはグループがデバイスまたはデバイス クラスへの書き込みアクセスを許可されている場合

    このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを拒否できます。

    例 3：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りアクセスを許可されている場合

    このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを許可できます。

    例 4：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りアクセスを拒否されている場合

このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、読み取りアクセスまたは読み取りおよび書き込みアクセスを許可できます。

例 5：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りおよび書き込みアクセスを許可されている場合

このユーザー、このグループ、またはこのグループのメンバーには、同じデバイスまたはデバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、書き込みアクセスまたは読み取りおよび書き込みアクセスを拒否できます。

例 6：ユーザーまたはグループがデバイスまたはデバイス クラスへの読み取りおよび書き込みアクセスを拒否されている場合

このユーザー、このグループ、またはこのグループのメンバーには、デバイス階層内でこのデバイスの下位にあるデバイスに対してのみ、読み取りアクセスまたは読み取りおよび書き込みアクセスを許可できます。

ユーザーまたはグループのアクセス拒否

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを拒否するには、以下の操作を行います。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - [**デバイス クラス**]
   - [**すべてのデバイス**]
   - [**個々のデバイス**]
3. [**ユーザー/グループ**]で、アクセスを拒否するユーザーまたはグループを選択し、[**拒否**]をクリックします。
4. [**適用**]をクリックします。

注記： 同じデバイス レベルでユーザーに対して拒否および許可を設定すると、アクセス許可よりもアクセス拒否が優先されます。

ユーザーまたはグループのアクセス許可

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを許可するには、以下の操作を行います。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスの一覧で、以下のどれかをクリックします。
   - [**デバイス クラス**]
   - [**すべてのデバイス**]
   - [**個々のデバイス**]
3. [**追加**]をクリックします。

[Select Users or Groups]（ユーザーまたはグループの選択）ダイアログ ボックスが表示されます。

4. [**詳細**]をクリックし、[**今すぐ検索**]をクリックして、追加するユーザーまたはグループを検索します。
5. 使用可能なユーザーおよびグループの一覧に追加するユーザーまたはグループをクリックして[**OK**]をクリックします。
6. 再度[**OK**]をクリックします。
7. [**許可**]をクリックして、そのユーザーによるアクセスを許可します。
8. [**適用**]をクリックします。

グループの単一ユーザーによるデバイス クラスへのアクセス許可

デバイス クラスへのアクセスを、グループ内のある 1 人のユーザーだけに許可して、同じグループ内の他のメンバーには拒否するには、以下の操作を行います。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - [**デバイス クラス**]
   - [**すべてのデバイス**]
   - [**個々のデバイス**]
3. [**ユーザー/グループ**]で、アクセスを拒否するグループを選択し、[**拒否**]をクリックします。
4. 目的のクラスの下のフォルダーに移動して、特定のユーザーを追加します。
5. [**許可**]をクリックして、そのユーザーによるアクセスを許可します。
6. [**適用**]をクリックします。

グループの単一ユーザーによる特定のデバイスへのアクセス許可

管理者は、特定のデバイスへのアクセスを、グループ内のある 1 人のユーザーだけに許可して、同じグループ内の他のメンバーには拒否することができます。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。
2. デバイスのリストで、設定するデバイス クラスをクリックして、その下のフォルダーに移動します。
3. [**ユーザー/グループ**]で、アクセスを許可するグループの横にある[**許可**]をクリックします。
4. アクセスを拒否するグループの横にある[**拒否**]をクリックします。
5. デバイス リストで、ユーザーによるアクセスを許可する特定のデバイスに移動します。
6. [**追加**]をクリックします。

   [Select Users or Groups]（ユーザーまたはグループの選択）ダイアログ ボックスが表示されます。

7. [**詳細**]をクリックし、[**今すぐ検索**]をクリックして、追加するユーザーまたはグループを検索します。

8. アクセスを許可するユーザーをクリックして[**OK**]をクリックします。

9. [**許可**]をクリックして、そのユーザーによるアクセスを許可します。

10. [**適用**]をクリックします。

ユーザーまたはグループの設定削除

ユーザーまたはグループによるデバイスまたはデバイス クラスへのアクセスを削除するには、以下の操作を行います。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。

2. デバイスの一覧で、設定するデバイス クラスをクリックします。
   - [**デバイス クラス**]
   - [**すべてのデバイス**]
   - [**個々のデバイス**]

3. [**ユーザー/グループ**]で、削除するユーザーまたはグループをクリックし、[**削除**]をクリックします。

4. [**適用**]をクリックします。

構成のリセット

⚠ **注意：** 構成をリセットすると、それまでに実行されたデバイスの構成変更がすべて破棄され、すべての設定が工場出荷時の設定値に戻ります。

構成設定を工場出荷時の値に戻すには、以下の操作を行います。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**デバイス クラス構成**]の順にクリックします。

2. [**リセット**]をクリックします。

3. 確認要求に対して[**はい**]をクリックします。

4. [**適用**]をクリックします。

ジャスト イン タイム認証の構成

ジャスト イン タイム認証の構成では、管理者はジャスト イン タイム認証（JITA）を使用してデバイスへのアクセスを許可されるユーザーおよびグループの一覧を表示したり変更したりできます。

ジャスト イン タイム認証が有効なユーザーは、[**デバイス クラス構成**]または[**簡易構成**]ビューで作成されたポリシーが制限されている一部のデバイスにアクセスできます。

- シナリオ：[簡易構成]ポリシーは、DVD ドライブや CD-ROM ドライブへのデバイス管理者以外のアクセスをすべて拒否するように構成されています。
- 結果：ジャスト イン タイム認証が有効なユーザーが DVD ドライブや CD-ROM ドライブにアクセスしようとすると、ジャスト イン タイム認証が有効になっていないユーザーと同じ「アクセ

ス拒否」メッセージが表示されます。次に、バルーン メッセージが表示され、ユーザーがジャスト イン タイム認証アクセスを希望するかどうかを尋ねます。バルーンをクリックすると、[Authenticate User]（ユーザー認証）ダイアログ ボックスが開きます。ユーザーが証明情報を正しく入力すると、DVD ドライブや CD-ROM ドライブへのアクセスが許可されます。

ジャスト イン タイム認証期間は、設定した時間（分）または 0 分の間有効です。ジャスト イン タイム認証期間を 0 分にすると、認証が有効のままになります。ユーザーは、認証されてからシステムからログオフするまで、デバイスにアクセスできます。

ジャスト イン タイム認証期間を延長するように構成することもできます。このシナリオでは、ジャスト イン タイム認証期間が失効する 1 分前に表示されるメッセージをクリックすることにより、再認証しなくてもアクセスを延長できるようにしています。

ユーザーに与えられるジャスト イン タイム認証期間が限定的か無制限かに関係なく、ユーザーがシステムをログオフしたり別のユーザーがログインしたりするとすぐに、ジャスト イン タイム認証期間は失効します。次にユーザーがログインし、ジャスト イン タイム認証が有効なデバイスにアクセスしようとすると、証明情報を入力するよう求めるメッセージが表示されます。

ジャスト イン タイム認証は以下のデバイス クラスに対して使用できます。

- DVD/CD-ROM ドライブ
- リムーバブル メディア

ユーザーまたはグループのジャスト イン タイム認証の作成

管理者は、ジャスト イン タイム認証を使用して、ユーザーまたはグループにデバイスへのアクセスを許可できます。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。
3. [+]をクリックして、ユーザーまたはグループをジャスト イン タイム認証の構成に追加します。
4. [**有効**]チェック ボックスにチェックを入れます。
5. ジャスト イン タイム認証の期間を必要な時間に設定します。
6. [**適用**]をクリックします。

新しいジャスト イン タイム認証の設定を適用するには、ユーザーはログアウトしてからログインしなおす必要があります。

ユーザーまたはグループの延長可能なジャスト イン タイム認証の作成

管理者は、ユーザーが失効前に延長できるジャスト イン タイム認証を使用して、ユーザーまたはグループにデバイスへのアクセスを許可できます。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。

3. [+]をクリックして、ユーザーまたはグループをジャスト イン タイム認証の構成に追加します。
4. [**有効**]チェック ボックスにチェックを入れます。
5. ジャスト イン タイム認証の期間を必要な時間に設定します。
6. [**延長可能**]チェック ボックスにチェックを入れます。
7. [**適用**]をクリックします。

新しいジャスト イン タイム認証の設定が適用されるには、ユーザーはログアウトして再びログインする必要があります。

ユーザーまたはグループのジャスト イン タイム認証の無効化

管理者は、ジャスト イン タイム認証を使用して、ユーザーまたはグループによるデバイスへのアクセスを無効にできます。

1. [HP ProtectTools 管理者コンソール]の左側の枠内で、[**Device Access Manager**]→[**ジャスト イン タイム認証の構成**]の順にクリックします。
2. デバイスのドロップダウン メニューから、[**リムーバブル メディア**]または[**DVD/CD-ROM ドライブ**]を選択します。
3. ジャスト イン タイム認証を無効にするユーザーまたはグループを選択します。
4. [**有効**]チェック ボックスのチェックを外します。
5. [**適用**]をクリックします。

ユーザーがログインし、デバイスにアクセスしようとすると、アクセスは拒否されます。

詳細設定

[詳細設定]には以下の機能があります。

- デバイス管理者グループの管理
- Device Access Manager によって常にアクセスが許可されるドライブ文字の管理

デバイス管理者グループは、（デバイス アクセスに関して）信頼できるユーザーを Device Access Manager ポリシーによる制限から除外するために使用されます。信頼できるユーザーには、通常、システム管理者が含まれます。詳しくは、98 ページの「デバイス管理者グループ」を参照してください。

[**詳細設定**]ビューで、管理者は Device Access Manager がどのユーザーに対してもアクセスを制限しないドライブ文字の一覧を構成することもできます。

注記： ドライブ文字の一覧が構成されるときは Device Access Manager のバックグラウンド サービスが実行されている必要があります。

これらのサービスを開始するには、以下の操作を行います。

1. リムーバブル メディアへのデバイス管理者以外のアクセスを拒否するなど、簡易構成ポリシーを適用します。

   または

   管理者権限でコマンド プロンプト ウィンドウを開き、以下のように入力します。

   sc start flcdlock

   enter キーを押します。

2. サービスが開始されると、ドライブ一覧を編集できるようになります。Device Access Manager で制御しないデバイスのドライブ文字を入力します。

   物理的なハード ディスクまたはパーティションのドライブ文字が表示されます。

   注記： システム ドライブ（通常は C）がこの一覧に含まれているかどうかに関係なく、システム ドライブへのアクセスはどのユーザーに対しても拒否されません。

デバイス管理者グループ

Device Access Manager をインストールすると、デバイス管理者グループが作成されます。

デバイス管理者グループは、（デバイス アクセスに関して）信頼できるユーザーを Device Access Manager ポリシーによる制限から除外するために使用されます。信頼できるユーザーには、通常、システム管理者が含まれます。

注記： ユーザーをデバイス管理者に追加しても、そのユーザーによるデバイスへのアクセスが自動的に許可されるわけではありません。[**デバイス クラス構成**]ビューで、Users グループがデバイスへのアクセスを拒否されている場合、デバイス管理者グループのメンバーがデバイスにアクセスできるようにするには、デバイス管理者グループによるアクセスが許可されている必要があります。ただし、[**簡易構成**]ビューを使用して、デバイス管理者グループのメンバーではないすべてのユーザーによるデバイス クラスへのアクセスを拒否できます。

ユーザーをデバイス管理者グループに追加するには、以下の操作を行います。

1. **[詳細設定]**ビューで、**[+]**をクリックします。
2. 信頼できるユーザーのユーザー名を入力します。
3. **[OK]**をクリックします。
4. **[適用]**をクリックします。

このグループのメンバーシップを管理するための別の方法は、以下のとおりです。

- Windows 7 Professional または Windows Vista の場合、標準の[ローカル ユーザーとグループ] Microsoft 管理コンソール（MMC）スナップインを使用して、このグループにユーザーを追加できます。
- Windows 7、Windows Vista、または Windows XP の各 Home Edition の場合は、管理者権限のあるアカウントからコマンド プロンプト ウィンドウで以下のように入力します。

  net localgroup “Device Administrators” ユーザー名 /add

  このコマンドで、「ユーザー名」は、このグループに追加するユーザーのユーザー名です。

eSATA サポート

Device Access Manager で eSATA デバイスを制御するには、以下を構成する必要があります。

1. システムの起動時にドライブが接続されている必要があります。
2. **[詳細設定]**ビューを使用して、Device Access Manager がアクセスを拒否しないドライブの一覧に eSATA ドライブ文字が含まれていないことを確認します。eSATA ドライブ文字が一覧に含まれている場合は、ドライブ文字を削除して**[適用]**をクリックします。
3. デバイスは、**[簡易構成]**ビューまたは**[デバイス クラス構成]**ビューで[リムーバブル メディア] デバイス クラスを使用して制御できます。

管理されないデバイス クラス

HP ProtectTools Device Access Manager では、以下のデバイス クラスは管理されません。

- 入出力デバイス
  - バイオメトリック（生体認証）
  - マウス
  - キーボード
  - プリンター
  - プラグ アンド プレイ（PnP）プリンター
  - プリンター アップグレード
  - 赤外線ヒューマン インターフェイス デバイス
  - スマート カード リーダー
  - マルチコネクタ シリアル

- ディスク ドライブ
    - フロッピー ディスク コントローラー（FDC）
    - ハード ディスク コントローラー（HDC）
    - ヒューマン インターフェイス デバイス（HID）クラス
- 電源
    - バッテリ
    - Advanced Power Management（APM）サポート
- その他
    - コンピューター
    - デコーダー
    - ディスプレイ
    - プロセッサ
    - システム
    - 不明
    - ボリューム
    - ボリューム スナップショット
    - セキュリティ デバイス
    - セキュリティ アクセラレーター
    - Intel®統合ディスプレイ ドライバー
    - メディア ドライバー
    - メディア チェンジャー
    - 多機能
    - Legacard
    - ネット クライアント
    - ネット サービス
    - ネット転送
    - SCSI アダプター

9 盗難からの回復

Computrace for HP ProtectTools（別売）を使用すると、コンピューターをリモートで監視、管理、および追跡できます。

Computrace for HP ProtectTools を有効にすると、Absolute Software Customer Center からツールの設定が行われます。管理者は Customer Center から Computrace for HP ProtectTools を設定し、コンピューターを監視または管理できます。システムの置き忘れや盗難が発生した場合、Customer Center はコンピューターを探索し取り戻すために地域当局に協力します。設定によって、ハードディスク ドライブが消去または交換された場合でも Computrace が動作し続けるようにすることができます。

Computrace for HP ProtectTools を有効にするには、以下の操作を行います。

1. インターネットに接続します。
2. ［**スタート**］→［**すべてのプログラム**］→［**HP**］→［**HP ProtectTools Security Manager**］の順にクリックします。
3. [HP ProtectTools Security Manager]の左側の枠内で、［**盗難からの回復**］をクリックします。
4. Computrace 有効化ウィザードを起動するには、［**今すぐ有効化**］をクリックします。
5. 連絡先情報とクレジット カードの支払い情報を入力するか、または事前に購入したプロダクト キーを入力します。

[有効化ウィザード]によって取引が安全に処理され、Absolute Software カスタマー センターの Web サイトにユーザー アカウントがセットアップされます。完了すると、カスタマー センターのアカウント情報を含む確認の電子メールが届きます。

以前に Computrace 有効化ウィザードを実行したことがあり、Customer Center ユーザー アカウントをすでに持っている場合は、HP のサポート窓口に問い合わせて追加ライセンスを購入できます。

カスタマー センターにログインするには、以下の操作を行います。

1. http://www.hp.com/ergo/から[日本語]を選択します。
2. ［**Login ID**］（ログイン ID）フィールドおよび［**Password**］（パスワード）フィールドに、確認の電子メールで受信した資格情報を入力し、［**Login**］（ログイン）をクリックします。

カスタマー センターでは、以下の操作を実行できます。

- コンピューターの監視
- リモート データの保護
- Computrace で保護されているコンピューターの盗難の報告

▲ Computrace for HP ProtectTools について詳しくは、[**詳細情報**]をクリックしてください。

10 Embedded Security for HP ProtectTools（一部のモデルのみ）

注記： Embedded Security for HP ProtectTools を使用するには、統合された TPM（Trusted Platform Module）セキュリティ チップがコンピュータに内蔵されている必要があります。

Embedded Security for HP ProtectTools は、ユーザ データや証明情報を不正なアクセスから保護します。このソフトウェア モジュールには、以下のセキュリティ機能があります。

- 高度な Microsoft EFS（Encryption File System）ファイルおよびフォルダの暗号化
- ユーザ データを保護するための PSD（Personal Secure Drive）の作成
- データ管理機能（キー階層のバックアップや復元など）
- Embedded Security ソフトウェアの使用時にデジタル証明情報の操作を保護するための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）のサポート

TPM 内蔵セキュリティ チップを使用すると、HP ProtectTools Security Manager の他のセキュリティ機能を強化したり有効にしたりできます。たとえば、Credential Manager for HP ProtectTools では、内蔵チップを Windows へのログオン時の認証要素として使用できます。

セットアップ手順

⚠ 注意： セキュリティ上の危険にさらされないようにするために、IT 管理者が内蔵セキュリティ チップをすぐに初期化することを強くおすすめします。内蔵セキュリティ チップを初期化しない場合、不正なユーザー、コンピューター ワーム、またはウィルスがコンピューターのオーナーシップを奪い、緊急リカバリ アーカイブの処理やユーザー アクセスの設定など所有者のタスクを制御してしまう可能性があります。

以下の項目の手順に沿って操作し、内蔵セキュリティ チップを有効にして初期化します。

[コンピューター セットアップ（F10）ユーティリティ]での内蔵セキュリティ チップの有効化

内蔵セキュリティ チップは、[Quick Initialization Wizard]（クイック初期化ウィザード）または[コンピューター セットアップ（F10）ユーティリティ]で有効にする必要があります。

[コンピューター セットアップ（F10）ユーティリティ]で内蔵セキュリティ チップを有効にするには、以下の操作を行います。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に[F10 = ROM Based Setup]（ROM ベースのセットアップ）というメッセージが表示されている間に f10 キーを押して、[コンピューター セットアップ（F10）ユーティリティ]を起動します。
2. 管理者パスワードを設定していない場合は、矢印キーを使用して［**Security**］（セキュリティ設定）→［**Setup password**］（セットアップ パスワード）の順に選択して enter キーを押します。
3. ［**New password**］（新しいパスワード）および［**Verify new password**］（新しいパスワードの確認）ボックスにパスワードを入力して f10 キーを押します。
4. ［**Security**］（セキュリティ設定）メニューで、矢印キーを使用して［**TPM Embedded Security**］（TPM 内蔵セキュリティ）を選択し、enter キーを押します。
5. ［**Embedded Security**］（内蔵セキュリティ）にデバイスが表示されない場合、［**Available**］（利用可能）を選択します。
6. ［**Embedded security device state**］（内蔵セキュリティ デバイスの状態）を選択し、設定を［**Enable**］（有効にする）に変更します。
7. f10 キーを押して、Embedded Security の設定への変更を確定します。
8. 設定を保存して[コンピューター セットアップ（F10）ユーティリティ]を終了するには、矢印キーを使用して［**File**］（ファイル）→［**Save Changes and Exit**］（変更を保存して終了）の順に選択し、画面の説明に沿って操作します。

内蔵セキュリティ チップの初期化

内蔵セキュリティの初期化プロセスでは、以下のことを行います。

- 内蔵セキュリティ チップの所有者のパスワードを設定します。これによって、内蔵セキュリティ チップ上のすべての所有者機能へのアクセスが保護されます。
- 緊急リカバリ アーカイブをセットアップします。緊急リカバリ アーカイブとは、すべてのユーザの基本ユーザ キーを再暗号化できるようにするための保護された記憶領域です。

内蔵セキュリティ チップを初期化するには、以下の手順で操作します。

1. タスク バーの右端の通知領域にある［**HP ProtectTools Security Manager**］（HP ProtectTools セキュリティ マネージャー）アイコンを右クリックして、［**Embedded Security Initialization**］（内蔵セキュリティの初期化）を選択します。

   [HP ProtectTools Embedded Security Initialization Wizard]（HP ProtectTools Embedded Security 初期化ウィザード）が起動します。

2. 画面に表示される説明に沿って操作します。

基本ユーザー アカウントのセットアップ

Embedded Security で基本ユーザ アカウントをセットアップすると、以下のタスクが実行されます。

- 暗号化された情報を保護するための基本ユーザ キーが生成され、その基本ユーザ キーを保護するための基本ユーザ キーのパスワードが設定されます。
- 暗号化されたファイルおよびフォルダを格納するための PSD（Personal Secure Drive）が設定されます。

注意： 基本ユーザ キーのパスワードは保護しておいてください。このパスワードがないと、暗号化されたデータにアクセスしたり復元したりできなくなります。

基本ユーザ アカウントをセットアップしてユーザ セキュリティ機能を有効にするには、以下の手順で操作します。

1. [Embedded Security User Initialization Wizard]（Embedded Security ユーザー初期化ウィザード）が起動していない場合は、**[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザの設定）の順にクリックします。
3. 右側のパネルで、**[Embedded Security Features]**（内蔵セキュリティの機能）の**[Configure]**（設定）をクリックします。

   [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

注記： セキュリティ保護された電子メールを使用するには、最初に、Embedded Security で作成されたデジタル証明情報を使用するように電子メール クライアントを設定する必要があります。デジタル証明情報が使用できない場合は、証明機関から取得する必要があります。電子メールを設定してデジタル証明情報を取得する手順については、電子メール クライアント ソフトウェアのヘルプを参照してください。

一般的なタスク

基本ユーザ アカウントのセットアップを完了すると、以下のタスクを実行できます。

- ファイルおよびフォルダの暗号化
- 暗号化された電子メールの送受信

Personal Secure Drive（PSD）の使用

PSD のセットアップを完了すると、次回のログオンで、基本ユーザ キーのパスワードを入力するよう要求されます。基本ユーザ キーのパスワードを正しく入力すると、Windows の[エクスプローラ]から直接 PSD にアクセスできます。

ファイルおよびフォルダの暗号化

暗号化ファイルを操作する場合は、以下の規則を考慮してください。

- 暗号化できるファイルおよびフォルダは、NTFS パーティション上のもののみです。FAT パーティション上のファイルおよびフォルダは暗号化できません。
- システム ファイルや圧縮されたファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時フォルダは、ハッカーの関心を引く可能性があるため、暗号化するようにしてください。
- ファイルまたはフォルダを初めて暗号化した時、回復ポリシーが自動的にセットアップされます。暗号化証明情報や秘密キーをなくした場合でも、このポリシーによって、回復エージェントを使用して情報の暗号化を解除できるようになります。

ファイルおよびフォルダを暗号化するには、以下の手順で操作します。

1. 暗号化するファイルまたはフォルダを右クリックします。
2. ［**Encrypt**］（暗号化）をクリックします。
3. 以下のオプションのどちらかをクリックします。
   - ［**Apply changes to this folder only**］（このフォルダにのみ変更を適用する）
   - ［**Apply changes to this folder, subfolders, and files**］（このフォルダ、およびサブフォルダとファイルに変更を適用する）
4. ［**OK**］をクリックします。

暗号化された電子メールの送受信

Embedded Security では、暗号化された電子メールの送受信を行うことができますが、その手順は電子メールのアクセスに使用しているプログラムによって異なります。詳しくは、Embedded Security ソフトウェアのヘルプおよび使用している電子メール アプリケーション ソフトウェアのヘルプを参照してください。

基本ユーザー キーのパスワードの変更

基本ユーザー キーのパスワードを変更するには、以下の操作を行います。

1. ［スタート］→［すべてのプログラム］→［**HP**］→［**HP ProtectTools Security Manager**］の順にクリックします。
2. 左側のパネルで、［**Embedded Security**］（内蔵セキュリティ）→［**User Settings**］（ユーザの設定）の順にクリックします。
3. 右側の枠内で、［**Basic User password**］（基本ユーザー パスワード）の［**Change**］（変更）をクリックします。
4. 古いパスワードを入力した後、新しいパスワードを設定して確定します。
5. ［**OK**］をクリックします。

高度なタスク

管理者は、Embedded Security 内で以下のタスクを実行できます。

- Embedded Security の証明情報、Embedded Security の設定、Personal Secure Drive のバックアップおよび復元
- 所有者のパスワードの変更
- ユーザー パスワードの再設定
- 移行元プラットフォームから移行先プラットフォームへの、ユーザー セキュリティ証明書の安全な移行

バックアップおよび復元

Embedded Security のバックアップ機能では、緊急の場合に復元される証明情報を含むアーカイブが作成されます。

バックアップ ファイルの作成

バックアップ ファイルを作成するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側の枠内で、**[Configure]**（設定）をクリックします。HP Embedded Security for ProtectTools Backup Wizard（HP Embedded Security for ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

バックアップ ファイルからの証明データの復元

バックアップ ファイルからデータを復元するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側の枠内で、**[Restore all]**（すべて復元）をクリックします。HP Embedded Security for ProtectTools Backup Wizard（HP Embedded Security for ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

所有者のパスワードの変更

管理者は、以下の操作を行って、所有者のパスワードを変更できます。

1. **[スタート]**→**[すべてのプログラム]**→**[すべてのプログラム]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Owner Password]**（所有者のパスワード）の**[Change]**（変更）をクリックします。
4. 古い所有者のパスワードを入力した後、新しい所有者のパスワードを設定して確定します。
5. **[OK]**をクリックします。

ユーザ パスワードの再設定

ユーザが忘れたパスワードを管理者に再設定してもらうことができます。詳しくは、ソフトウェアのヘルプを参照してください。

移行ウィザードによるキーの移行

移行は、キーや証明情報の管理、復元、転送などを行うことができる、高度な管理者タスクです。

移行について詳しくは、Embedded Security ソフトウェアのヘルプを参照してください。

11　ローカライズされたパスワードの例外事項

ブート前セキュリティ レベルおよび HP Drive Encryption レベルでは、以下の項目で説明しているように、パスワードのローカライズのサポートに制限があります。

Windows IME はブート前セキュリティ レベルまたは HP Drive Encryption レベルではサポートされない

Windows では、IME（入力方式エディター）を選択することによって、日本語や中国語の文字などの複雑な文字および記号を、一般的な西洋言語用のキーボードを使用して入力できます。

IME は、ブート前セキュリティ レベルまたは HP Drive Encryption レベルではサポートされていません。ブート前セキュリティまたは HP Drive Encryption のログイン画面では、IME を使用して Windows パスワードを入力することはできません。また、入力しようとすると、ロックアウトが発生することがあります。場合によっては、パスワードの入力時に Microsoft Windows によって IME が表示されないこともあります。

たとえば、一部の Windows XP 日本語版インストール環境では、初期設定の IME は、日本語 Microsoft IME Standard 2002 と呼ばれています。日本語 Microsoft IME Standard 2002 は、実際にはキーボード レイアウト E0010411 に変換されます。ただし、日本語 Microsoft IME Standard 2002 は IME であり、キーボード レイアウトではありません（Microsoft によって、IME 用にキーボード レイアウトのコーディング スキームが予約されており、キーボード レイアウトの概念が拡大されています）。日本語 Microsoft IME Standard 2002 は、BIOS ブート前セキュリティ パスワードのプロンプト、または HP Drive Encryption パスワードのプロンプトの入力環境で使用できるキーボード レイアウトではないため、この IME を使用して入力したパスワードは HP ProtectTools によって拒否されます。また、日本語 Microsoft IME Standard 2002 は、Microsoft Windows Vista®の「共通名」とも異なります。Windows は一部の IME をキーボード レイアウトにマッピングします。このような場合、HP ProtectTools は IME をサポートします。これは、元となっているキーボード レイアウトの定義（16 進数コード）が使用されているためです。

この問題を解決するには、サポートされている以下のどれかのキーボード レイアウトに切り替えます。これらのキーボード レイアウトは、キーボード レイアウト 00000411 に変換されます。

- 日本語 Microsoft IME
- 日本語キーボード レイアウト
- Office 2007 IME（日本語）: Microsoft や他社が、IME または入力方式エディターという用語を使用している場合、その入力方式は実際には IME ではないことがあります。このため、混乱が生じることもありますが、ソフトウェアは 16 進表記を読み取ります。したがって、サポートされているキーボード レイアウトに IME がマッピングされている場合、HP ProtectTools はその設定をサポートできます。

⚠ **警告！** HP ProtectTools を使用すると、Windows IME を使用して入力したパスワードは拒否されます。

サポートされている別のキーボード レイアウトを使用したパスワードの変更

初期パスワードをあるキーボード レイアウト（たとえば、英語（米国）（409））を使用して設定し、後から、サポートされている別のキーボード レイアウト（たとえば、ラテン アメリカ言語（080A））を使用して変更すると、そのパスワードの変更は HP Drive Encryption では正常に認識されます。ただし、ラテン アメリカ言語に存在して、英語（米国）には存在しない文字（たとえば、ē）を使用すると、BIOS では正常に認識されません。

注記： 管理者はこの問題を解決できます。[HP ProtectTools ユーザーの管理]機能を使用して、HP ProtectTools からこのユーザーを削除し、オペレーティング システムで目的のキーボード レイアウトを選択してから、同じユーザーに対して Security Manager セットアップ ウィザードを実行しなおします。BIOS に目的のキーボード レイアウトが保存され、このキーボード レイアウトを使用して入力できるパスワードが BIOS 内に適切に設定されます。

もう 1 つ問題になる可能性があるのが、同じ文字を出力できる、異なるキーボード レイアウトを使用している場合です。たとえば、米国インターナショナル キーボード レイアウト（20409）とラテン アメリカ言語キーボード レイアウト（080A）は、どちらも文字 é を出力できますが、異なる順序でキーを操作しなければならないことがあります。最初にラテン アメリカ言語キーボード レイアウトを使用してパスワードを設定すると、その後に米国インターナショナル キーボード レイアウトを使用してパスワードを変更しても、BIOS にはラテン アメリカ言語キーボード レイアウトが設定されます。

特別なキーの扱い

- 中国語、スロバキア語、カナダ フランス語、およびチェコ語

  上記のキーボード レイアウトのどれかを選択してパスワードを入力した場合（たとえば、abcdef）、BIOS ブート前セキュリティおよび HP Drive Encryption では、同じパスワードを小文字の場合は shift キーを押しながら、大文字の場合は shift キーと caps lock キーを押しながら入力する必要があります。数字のパスワードは、テンキーを使用して入力する必要があります。

- 韓国語

  サポートされている韓国語キーボード レイアウトを選択してパスワードを入力した場合、BIOS ブート前セキュリティおよび HP Drive Encryption では、同じパスワードを小文字の場合は右 alt キーを押しながら、大文字の場合は右 alt キーと caps lock キーを押しながら入力する必要があります。

- サポートされていない文字は、以下の表のとおりです。

言語	Windows	BIOS	Drive Encryption
アラビア語	ﻹ、ﻵ、およびﻻキーは、2 文字になります	ﻹ、ﻵ、およびﻻキーは、1 文字になります	ﻹ、ﻵ、およびﻻキーは、1 文字になります
カナダ フランス語	caps lock を押した状態で入力した ç、è、à、および é は、Windows では Ç、È、À、および É になります	caps lock を押した状態で入力した ç、è、à、および é は、BIOS ブート前セキュリティでは ç、è、à、および é になります	caps lock を押した状態で入力した ç、è、à、および é は、HP Drive Encryption では ç、è、à、および é になります
スペイン語	40a はサポートされていません。ただし、ソフトウェアによって c0a に変換されるため、40a は正常に動作します。しかし、これらのキーボード レイアウトはわずかに異なるため、スペイン語を話すユーザーは、Windows のキーボード レイアウトを 1040a（スペイン語（バリエーション））または 080a（ラテン アメリカ言語）に変更することをおすすめします	n/a	n/a
米国インターナショナル	◦ 1 番上の行にある¡、¤、‘、’、¥、および×キーは拒否されます ◦ 2 番目の行にある å、®、および þ キーは拒否されます ◦ 3 番目の行にある á、ð、および ø キーは拒否されます ◦ 1 番下の行にある æ キーは拒否されます	n/a	n/a

言語	Windows	BIOS	Drive Encryption
チェコ語	◦ ğ キーは拒否されます ◦ į キーは拒否されます ◦ ų キーは拒否されます ◦ ė、ı、および ż キーは拒否されます ◦ ģ、ķ、ļ、ņ、および ŗ キーは拒否されます	n/a	n/a
スロバキア語	ż キーは拒否されます	◦ š、ś、および ş キーは、入力した場合は拒否されますが、ソフト キーボードを使用して入力した場合は受け入れられます ◦ ţ デッド キーは 2 文字になります	n/a
ハンガリー語	ż キーは拒否されます	ţ キーは 2 文字になります	n/a
スロベニア語	żŻ キーは Windows では拒否されます。また、alt キーは、BIOS ではデッド キーとなります	ú、Ú、ů、Ů、ş、Ş、ś、Ś、š、および Š キーは、BIOS では拒否されます	n/a
日本語	Windows XP の場合のみ、標準の日本語キーボードレイアウトである 411 が完全にサポートされます。Windows XP で通常「Microsoft Standard IME 2002」と表示される IME は、通常はサポートされません。ただし、単純な文字を入力している場合、この IME はキーボード レイアウト 411 とほぼ同じであることが、テストからわかっています。したがって、ローカライズされた日本語パスワードを使用して BIOS および HP Drive Encryption を保護している場合、この IME は、ソフトウェアによってキーボード レイアウト 411 に切り替えられます 利用できる場合は、Microsoft Office 2007 IME を選択することをおすすめします。IME という名前は付いていますが、実際にはキーボード レイアウト 411 であり、サポートされています	n/a	n/a

パスワードが拒否された場合の対処方法

パスワードは、以下の原因で拒否されることがあります。

- サポートされていない IME をユーザーが使用している場合。これは、2 バイト文字言語（韓国語、日本語、中国語）ではよく起こる問題です。この問題を解決するには、以下の操作を行います。
  1. [**スタート**]→[**コントロール パネル**]→[**地域と言語のオプション**]の順にクリックします。
  2. [**言語**]タブをクリックします。
  3. [**詳細**]ボタンをクリックします。
  4. [**設定**]タブで、[**追加**]ボタンをクリックして、サポートされているキーボードを追加します（[入力言語]の[中国語]の下で、[US]キーボードを追加します）。
  5. サポートされているキーボードを初期の入力言語に設定します。
  6. HP ProtectTools を再起動してから、パスワードを入力しなおします。
- ユーザーがサポートされていない文字を使用している場合。この問題を解決するには、以下の操作を行います。
  1. サポートされている文字のみを使用するように Windows パスワードを変更します。サポートされていない文字は、115 ページの「特別なキーの扱い」のとおりです。
  2. Security Manager セットアップ ウィザードを再度実行し、新しい Windows パスワードを入力します。

用語集

ATM
Automatic Technology Manager。ネットワーク管理者がシステムを BIOS レベルでリモート管理できます。

Drive Encryption
ハードドライブを暗号化して、適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護します。

Drive Encryption のログオン画面
Windows が起動する前に表示されるログオン画面。ユーザーは、Windows のユーザー名およびパスワード、またはスマート カード PIN を入力する必要があります。ほとんどの場合、Drive Encryption のログオン画面で正しい情報を入力すれば、Windows のログオン画面で再度ログオンすることなく、直接 Windows にアクセスできます。

DriveLock
ハードドライブをユーザーにリンクして、コンピューターの起動時にユーザーに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

HP SpareKey
Drive Encryption キーのバックアップ コピー。

ID
HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）内で、特定のユーザーのアカウントまたはプロファイルのように処理される、証明情報と設定の集合。

ID カード
ユーザー名および選択された画像を使用してデスクトップを視覚的に識別するための、Windows デスクトップのガジェット。HP ProtectTools 管理者コンソールを開くには、ID カードをクリックします。

JITA
ジャスト イン タイム認証。

PIN
個人識別番号。

PKI
証明情報および暗号化キーを作成、使用、および管理するためのインターフェイスを定義する、公開キー基盤の規格。

Privacy Manager の証明書
電子メール メッセージおよび Microsoft Office ドキュメントに対する署名や暗号化など、暗号の演算に使用するたびに認証が必要なデジタル証明書。

PSD
Personal Secure Drive。機密情報を保護するための記憶領域を提供する機能。

SATA device mode（SATA デバイス モード）
コンピューターと大容量ストレージ デバイス（ハードドライブやオプティカル ドライブなど）の間のデータ転送モード。

Trusted Platform Module（トラステッド プラットフォーム モジュール）内蔵セキュリティ チップ
HP ProtectTools Embedded Security チップの一般的な呼び方。TPM では、ホスト システムに固有の情報（暗号化キー、デジタル署名、パスワードなど）が格納され、ユーザーではなくコンピューターが認証されます。TPM を使用すると、物理的な盗難や外部のハッカーによる攻撃によってコンピューター上の情報が危険にさらされるリスクを最小限に抑えることができます。

TXT
Trusted Execution Technology（トラステッド エグゼキューション テクノロジ）の略。

USB トークン
ユーザーに関する識別情報が格納されているセキュリティ デバイス。スマート カードや指紋認証システムと同様に、所有者をコンピューターに対して認証するために使用されます。

Windows 管理者
アクセス権を変更し、他のユーザーを管理するすべての権限を持つユーザー。

Windows ユーザー アカウント
ネットワークまたは個別のコンピューターへのログオンを承認された個人のプロファイル。

Windows ログオンのセキュリティ
アクセスのために特定の証明情報を使用するよう求めることで、Windows アカウントを保護できます。

空き領域ブリーチ
削除されたフォルダーやファイルにランダムなデータを安全に上書きして、削除されたフォルダーやファイルの元の内容をわからなくすることです。

暗号化
権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号化サービス プロバイダー（CSP）
明確なインターフェイスを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除
暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）
選択されたフォルダー内のすべてのファイルおよびサブフォルダーを暗号化するシステム。

暗号法
特定の個人のみが解読できるように、データを暗号化および暗号化解除する手法。

[安全に送信]ボタン
[Microsoft Outlook]の電子メール メッセージのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、[Microsoft Outlook]の電子メール メッセージに対する署名や暗号化ができます。

移行
Privacy Manager の証明書および信頼済み連絡先を管理、復元、および転送する作業。

仮想トークン

スマート カードやカード リーダーとよく似た働きをするセキュリティ機能。このトークンは、コンピューターのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザー PIN の入力を要求されます。

管理者
「Windows 管理者」を参照してください。

キーの組み合わせ
特定のキーの組み合わせ。ctrl ＋ alt ＋ s キーなどを押すと、自動シュレッドが開始されます。

緊急リカバリ アーカイブ
他のプラットフォームの所有者キーを使用して基本ユーザー キーを再暗号化できる、保護された記憶領域。

グループ
デバイス クラスまたは特定のデバイスに対して同じレベルのアクセス許可またはアクセス拒否が設定されているユーザーのグループ。

コンソール
HP ProtectTools 管理者コンソールの機能および設定に対するアクセスや管理を行うことができる、中心となる場所。

シーン
登録されたユーザーの認証に使用する写真。

自動シュレッド
ユーザーが File Sanitizer で設定したスケジュールに従って実行されるシュレッドのことです。

指紋
指紋の画像をデジタルの形式で抽出したもの。実際の指紋の画像は、HP ProtectTools Security Manager には保存されません。

手動シュレッド
単一のフォルダーやファイルまたは選択されている複数のフォルダーやファイルに対して、自動シュレッド スケジュールを省略して実行されるシュレッド。

シュレッド
フォルダーやファイルに含まれるデータの内容をわからなくするアルゴリズムの実行。

シュレッド サイクル
各フォルダーやファイルでシュレッド アルゴリズムを実行する回数。選択したシュレッド サイクルの回数が多いほど、コンピューターのセキュリティは高くなります。

シュレッド プロファイル
あらかじめ指定されている消去方法とフォルダーやファイルの一覧。

証明情報
ユーザーが認証プロセスで特定のタスクに対する適格性を証明するための手段。

[署名と暗号化]ボタン
Microsoft Office アプリケーションのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、Microsoft Office ドキュメントに対する署名、暗号化、または暗号化の解除ができます。

署名欄
デジタル署名を表示するためのプレースホルダー。ドキュメントに署名すると、署名者の名前と確認方法が表示されます。署名日と署名者のタイトルも表示できます。

シングルサインオン

認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに HP ProtectTools Security Manager を使用してアクセスできるようにする機能。

シンプル削除
Windows のフォルダーやファイルの参照情報の削除。空き領域ブリーチを実行しても、フォルダーやファイルの内容をわからなくするデータをフォルダーやファイルに上書きしないかぎり、そのフォルダーやファイルの内容はハードドライブ上に残ります。

信頼済み連絡先
信頼済み連絡先への招待を承認した人物。

信頼済み連絡先宛てに封印
電子メールにデジタル署名を付加した上で暗号化し、選択したセキュリティ ログオン方法による認証の後に送信する作業。

信頼済み連絡先の一覧
信頼済み連絡先の一覧。

信頼済み連絡先の受信者
信頼済み連絡先になるための招待を受け取った人物。

信頼済み連絡先への招待状
信頼済み連絡先になることを依頼するために送信された電子メール。

信頼できる送信者
署名および暗号化した電子メールや Microsoft Office ドキュメントを送信する信頼済み連絡先。

信頼できるメッセージ
信頼できる送信者から信頼済み連絡先に宛てて、信頼できるメッセージを送信する通信セッション。

推奨する署名者
ドキュメントに署名欄を追加するために[Microsoft Word]または[Microsoft Excel]ドキュメントの所有者が指名したユーザー。

スマート カード
所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピューターに対して認証するために使用されます。

セキュリティ ログオン方法
コンピューターへのログオンに使用される方法。

ダッシュボード
Security Manager for HP ProtectTools の機能および設定に対するアクセスや管理を行うことができる、中心となる場所。

デジタル証明書
デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

デジタル署名
資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

デバイス アクセス制御ポリシー
ユーザーがアクセスを許可または拒否されているデバイスの一覧。

デバイス クラス
ドライブなど、特定の種類にあてはまるすべてのデバイス。

電源投入時認証
スマート カード、セキュリティ チップ、パスワードなど、コンピューターの起動時に何らかの形式の認証を要求するセキュリティ機能。

トークン
「セキュリティ ログオン方法」を参照してください。

ドメイン
ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピューターの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

認証
ユーザーがタスクの実行（コンピューターへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

認証機関（CA）
公開キー基盤の運営に必要な証明書を発行するサービス。

ネットワーク アカウント
ローカル コンピューター上、ワークグループ内、またはドメイン上の Windows ユーザーまたは管理者のアカウント。

バイオメトリック（生体認証）
指紋などの身体的な特徴を使用してユーザーを識別する認証証明のカテゴリ。

廃止パスワード
ユーザーがデジタル証明書を要求するときに作成されるパスワード。このパスワードは、ユーザーがデジタル証明書を廃止する場合に必要です。これによって、ユーザー自身のみが証明書を廃止できるようになります。

バックアップ
バックアップ機能を使用して、重要なプログラム情報のコピーをそのプログラムの外部の場所に保存すること。バックアップした内容は、後日、同じコンピューターまたは別のコンピューターに情報を復元するために使用できます。

バックグラウンド サービス
デバイス アクセス制御ポリシーを適用するには、[HP ProtectTools デバイス ロック/検査]バックグラウンド サービスが実行されている必要があります。このサービスは、[コントロール パネル]の[管理ツール]オプションにある[サービス]アプリケーションで確認できます。このサービスが実行されていない場合、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）は、デバイス アクセス制御ポリシーが適用されているときにサービスを起動しようと試みます。

フォルダー/ファイル
個人の情報やファイル、履歴や Web 関連のデータなどを含むデータ コンポーネントのことで、ハードドライブ上に存在します。

復元
プログラム情報を、以前に保存されたバックアップ ファイルからこのプログラムにコピーするプロセス。

有効化
Drive Encryption の機能にアクセスする前に完了する必要があるタスク。Drive Encryption は、HP ProtectTools セットアップ ウィザードを使用して有効にします。管理者のみが Drive Encryption を有効にできます。有効化プロセスは、ソフトウェアの有効化、ドライブの暗号化、ユーザー アカウントの作成、およびリムーバブル ストレージ デバイス上の初期バックアップ暗号化キーの作成で構成されます。

ユーザー
Drive Encryption に登録された人。管理者以外のユーザーは、Drive Encryption での権限が制限されています。管理者以外のユーザーが実行できる操作は、登録（管理者の許可がある場合）とログオンのみです。

リブート
コンピューターを再起動するプロセス。

ログオン
Web サイトやその他のプログラムにログオンするために使用できるユーザー名とパスワード（またはその他の選択された情報）で構成される、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャー）内のオブジェクト。

索引

す

せ

そ

た

つ

て